ExtremeXOS Installation and Release Notes

Software Version ExtremeXOS 12.1.4-patch1-9

Extreme Networks, Inc.
3585 Monroe Street
Santa Clara, California 95051
(888) 257-3000
(408) 579-2800
http://www.extremenetworks.com

Published: August 2010
Part Number: 120415-00 Rev 45

AccessAdapt, Alpine, Altitude, BlackDiamond, EPICenter, ExtremeWorks Essentials, Ethernet Everywhere, Extreme Enabled, Extreme Ethernet Everywhere, Extreme Networks, Extreme Standby Router Protocol, Extreme Turbodrive, Extreme Velocity, ExtremeWare, ExtremeWorks, ExtremeXOS, Go Purple Extreme Solution, ExtremeXOS ScreenPlay, ReachNXT, Sentriant, ServiceWatch, Summit, SummitStack, Triumph, Unified Access Architecture, Unified Access RF Manager, UniStack, the Extreme Networks logo, the Alpine logo, the BlackDiamond logo, the Extreme Turbodrive logo, the Summit logos, and the Powered by ExtremeXOS logo are trademarks or registered trademarks of Extreme Networks, Inc. or its subsidiaries in the United States and/or other countries.

sFlow is a registered trademark of InMon Corporation.

Specifications are subject to change without notice.

All other registered trademarks, trademarks, and service marks are property of their respective owners.

© 2010 Extreme Networks, Inc. All Rights Reserved.

Contents

Chapter 1: Overview 5

Configuration Change in ExtremeXOS 12.1 5
Feature Enhancements in ExtremeXOS 12.1.3 5
BGP Enhancements 5
Flow Control—Summit Family of Switches and BlackDiamond 8800 Series Switches Only 32
STP and Network Login 45
Health Check Link Aggregation 47
New FEFI CLI Command 64
New Features or Feature Enhancements in ExtremeXOS 12.1.2.17 66
New Hardware Supported in ExtremeXOS 12.1.2.17 66
New Features in ExtremeXOS 12.1 67
New Hardware Supported in ExtremeXOS 12.1.1.4 69
Supported Hardware 69
BlackDiamond 10808 Switch Component Support 69
BlackDiamond 8800 Series of Switches Component Support 71
BlackDiamond 12800 Series Switches Component Support 72
Summit X150 and X350 Component Support 72
Summit X250e Component Support 72
Summit X450 Component Support 73
SFP (Mini-GBIC) Support 74
XENPAK Module Support 77
XFP Module Support 79
Summit X150 and X350 Series Switch Software Details 80
ExtremeXOS Command Line Support 81
Supported Commands on the Summit X150 and X350 Series Switches 81
Unsupported Commands on the Summit X150 and X350 Series Switches 92
Tested Third-Party Products 94
Tested RADIUS Servers 94
Tested Third-Party Clients 94
PoE Capable VoIP Phones 94
Extreme Switch Security Assessment 95
DoS Attack Assessment 95
ICMP Attack Assessment 95
Port Scan Assessment 95

Chapter 2: Upgrading to ExtremeXOS 12.1 97

Staying Current 97
Upgrading ExtremeXOS 97
Quick Summary 98
Detailed Steps 99
Upgrading ExtremeXOS on a Summit X150 and X350 103
Upgrading ExtremeXOS on a Summit X250e 104
Upgrading ExtremeXOS on a Summit X450 105
Upgrading an MSM-5 and MSM-5R to ExtremeXOS 12.1 on a BlackDiamond 12802 105

Upgrading a BlackDiamond Series of Switches Using Hitless Upgrade....107
Upgrading the Alternate Partition Using Hitless Upgrade....107
Dual MSM Systems with Different Images Present....108
Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL....109
Installing an ExtremeXOS Module....110
Uninstalling an SSH Module....111
Downgrading Switches....111

Chapter 3: Limits....113

Supported Limits....113

Chapter 4: Open Issues, Known Behaviors, and Resolved Issues....133

Open Issues....134
Known Behaviors....148
Resolved Issues in ExtremeXOS 12.1.4-patch1-9....153
Resolved Issues in ExtremeXOS 12.1.4-patch1-8....153
Resolved Issues in ExtremeXOS 12.1.4-patch1-7....154
Resolved Issues in ExtremeXOS 12.1.4-patch1-6....154
Resolved Issues in ExtremeXOS 12.1.4-patch1-5....155
Resolved Issues in ExtremeXOS 12.1.4-patch1-4....155
Resolved Issues in ExtremeXOS 12.1.4-patch1-3....156
Resolved Issues in ExtremeXOS 12.1.4-patch1-2....156
Resolved Issues in ExtremeXOS 12.1.4-patch1-1....157
Resolved Issues in ExtremeXOS 12.1.4....158
Resolved Issues in ExtremeXOS 12.1.3-patch1-9....159
Resolved Issues in ExtremeXOS 12.1.3-patch1-8....160
Resolved Issues in ExtremeXOS 12.1.3-patch1-6....161
Resolved Issues in ExtremeXOS 12.1.3-patch1-4....163
Resolved Issues in ExtremeXOS 12.1.3-patch1-2....165
Resolved Issues in ExtremeXOS 12.1.3....167
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-17....170
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-15....171
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-12....172
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-10....173
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-7....174
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-4....174
Resolved Issues in ExtremeXOS 12.1.2.17-patch1-3....176
Resolved Issues in ExtremeXOS 12.1.2.17....177
Resolved Issues in ExtremeXOS 12.1.1.4....180
Resolved Issues in ExtremeXOS 12.1.0.29....183

1 Overview

These Release Notes document ExtremeXOS® 12.1.4-patch1-9.

This chapter contains the following sections:

- Configuration Change in ExtremeXOS 12.1 on page 5
- Feature Enhancements in ExtremeXOS 12.1.3 on page 5
  - BGP Enhancements on page 5
  - Flow Control—Summit Family of Switches and BlackDiamond 8800 Series Switches Only on page 32
  - STP and Network Login on page 45
  - Health Check Link Aggregation on page 47
  - New FEFI CLI Command on page 64
- New Features or Feature Enhancements in ExtremeXOS 12.1.2.17 on page 66
- New Features in ExtremeXOS 12.1 on page 67
- New Hardware Supported in ExtremeXOS 12.1.1.4 on page 69
- Supported Hardware on page 69
- Summit X150 and X350 Series Switch Software Details on page 80
- Tested Third-Party Products on page 94
- Extreme Switch Security Assessment on page 95

Configuration Change in ExtremeXOS 12.1

While loading a configuration from a pre ExtremeXOS 12.1 release, and having an ip-mtu greater than 9,194, the value is reduced to 9,194 after upgrading to ExtremeXOS 12.1 or later. You will not receive a log message notification of this value reduction.

Feature Enhancements in ExtremeXOS 12.1.3

Following are the feature enhancements supported in ExtremeXOS 12.1.3. These features will be documented in detail in the ExtremeXOS 12.3 versions of the *ExtremeXOS Concepts Guide* and the *ExtremeXOS Command Reference Guide*, unless otherwise noted.

BGP Enhancements

The following new BGP features have been added in this release:

- Inactive Route Advertisement on page 6
- Default Route Origination and Advertisement on page 10

- BGP ECMP on page 19
- Support for Overlapping Aggregate Routes on page 25
- Blackhole Route Redistribution on page 27

Inactive Route Advertisement

BGP inactive routes are defined as those routes that are rated *best* by BGP and *not best* in IP routing table. For example, an IGP route to the same destination may be best because it has a higher priority in the IP route table than the BGP best route. The default configuration of the ExtremeXOS software does not advertise BGP inactive routes to BGP neighbors.

The default configuration (no BGP inactive route advertisement) is more consistent with data traffic forwarding. However, when advertisement of inactive BGP routes is enabled, BGP need not depend upon the route manager module to know whether a BGP route is active or not. This actually improves the performance of BGP processing and advertisement.

To enable or disable BGP inactive route advertising, use the following commands:

```
enable bgp {address-family [ipv4-unicast | ipv4-multicast]} advertise-inactive-route
disable bgp {address-family [ipv4-unicast | ipv4-multicast]} advertise-inactive-route
```

When BGP inactive route advertising is enabled, inactive BGP routes are considered for BGP route aggregation. When this feature is disabled, inactive BGP routes are ignored while aggregating routes.

The following commands have been added or modified to support this feature:

- disable bgp advertise-inactive-route on page 7
- enable bgp advertise-inactive-route on page 8
- show bgp on page 9

disable bgp advertise-inactive-route

```
disable bgp {address-family [ipv4-unicast | ipv4-multicast]} advertise-
inactive-route
```

Description

Disables advertisement of BGP inactive routes, which are defined as those routes that rated *best* by BGP and *not best* in the IP routing table.

Syntax Description

ipv4-unicast	Disables inactive route advertisement for IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Disables inactive route advertisement for IPv4 multicast routes.

Default

Disabled.

Usage Guidelines

This command can be successfully executed only when BGP is globally disabled. If you want to disable inactive route advertisement and BGP is enabled, you must disable BGP (`disable bgp`), disable this feature, and then enable BGP (`enable bgp`).

Example

The following command disables inactive route advertisement for IPv4 unicast traffic:

```
disable bgp address-family ipv4-unicast advertise-inactive-route
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

enable bgp advertise-inactive-route

```
enable bgp {address-family [ipv4-unicast | ipv4-multicast]} advertise-
inactive-route
```

Description

Enables advertisement of BGP inactive routes, which are defined as those routes that rated *best* by BGP and *not best* in the IP routing table.

Syntax Description

ipv4-unicast	Enables inactive route advertisement for IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Enables inactive route advertisement for IPv4 multicast routes.

Default

Disabled.

Usage Guidelines

This command can be successfully executed only when BGP is globally disabled. It is best to enable this feature before you enable BGP (`enable bgp`). If BGP is enabled, you must disable BGP (`disable bgp`), enable this feature, and then enable BGP.

Example

The following command enables inactive route advertisement for IPv4 unicast traffic:

```
enable bgp address-family ipv4-unicast advertise-inactive-route
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

show bgp

```
show bgp
```

Description

Displays BGP configuration information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays BGP configuration information:

```
# show bgp

Enabled             : Yes               OperStatus          : Up
RouterId            : 10.203.134.73     As                  : 100
LocalPref           : 100               MED                 : None
Always-Compare-MED  : Disabled          Aggregation         : Disabled
Route Reflector     : No                RR ClusterId        : 0
IGP Synchronization : Disabled          New Community Format: Disabled
Routes from EBGP    : 2                 Routes from IBGP    : 0
Routes redistributed: 0                 Out Updates queued  : 0
Fast Ext Fallover   : Disabled          MPLS LSP as Next-Hop: No
ConfedId            : 0                 Maximum ECMP Paths  : 5
Confed Peers        :
Networks            : 0
Aggregate Networks  : 0
Redistribute:
  ipv4       Admin     Operational  Shutdown  Policy
  unicast    Status    Status       Priority
  ------------------------------------------------------
  Direct     Disabled  Down         2048      None
  Static     Disabled  Down         2048      None
  RIP        Disabled  Down         2048      None
  OSPFIntra  Disabled  Down         2048      None
  OSPFInter  Disabled  Down         2048      None
  OSPFExt1   Disabled  Down         2048      None
  OSPFExt2   Disabled  Down         2048      None
  ISISL1     Disabled  Down         2048      None
```

```
  ISISL2      Disabled  Down          2048      None
  ISISL1Ext   Disabled  Down          2048      None
  ISISL2Ext   Disabled  Down          2048      None

  ipv4        Admin     Operational   Shutdown  Policy
  multicast   Status    Status        Priority
  ------------------------------------------------------
  Direct      Disabled  Down          2048      None
  Static      Disabled  Down          2048      None
  RIP         Disabled  Down          2048      None
  OSPFIntra   Disabled  Down          2048      None
  OSPFInter   Disabled  Down          2048      None
  OSPFExt1    Disabled  Down          2048      None
  OSPFExt2    Disabled  Down          2048      None
  ISISL1      Disabled  Down          2048      None
  ISISL2      Disabled  Down          2048      None
  ISISL1Ext   Disabled  Down          2048      None
  ISISL2Ext   Disabled  Down          2048      None
Advertise Inactive Routes:
  ipv4-unicast   : Disabled
  ipv4-multicast : Disabled
```

History

This command was first available in ExtremeXOS 10.1.

This command required a specific license in ExtremeXOS 11.1.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

Default Route Origination and Advertisement

The default route origination and advertisement feature allows you to originate and advertise a default route to a BGP neighbor (or to all neighbors in a peer group) even though no default route exists in the local IP routing table. It also allows you to associate policy rules to *conditionally* advertise a default route to BGP neighbors.

When default route origination becomes active, the default route is advertised to the specified BGP neighbors, overriding any previously sent default route. If a default route is added to the local IP routing table while default route origination is active, the default route defined by this feature takes precedence over the new *regular* default route. If default route origination becomes inactive, and a regular default route exists, the regular default route is advertised to BGP neighbors.

The following sections provide additional information on this feature:

- Managing Policies for Default Route Origination on page 11
- Enabling and Disabling Route Origination on page 11
- Example: Default Route Origination on page 11

Managing Policies for Default Route Origination

When you use a policy with default route origination, the default route is originated only if the local BGP RIB contains a route that matches the policy match conditions. You can use the following match conditions:

- NLRI
- AS-path
- Community
- Origin

You can also use the following policy actions in the policy to set the route attributes:

- AS-path
- Community
- Origin

After a policy is configured for default route origination, BGP must periodically scan the local BGP RIB to make sure that the policy rules evaluate to true for at least one route in local BGP RIB. If the rules evaluate to true, default origination remains active. If the rules evaluate to false, then default origination becomes inactive and the default routes must be withdrawn.

Enabling and Disabling Route Origination

To enable or disable BGP default route origination and advertisement for BGP neighbors, use the following commands:

```
enable bgp [{neighbor} <remoteaddr> | neighbor all] {address-family [ipv4-unicast |
ipv4-multicast]} originate-default {policy <policy-name>}
disable bgp [{neighbor} <remoteaddr> | neighbor all] {address-family [ipv4-unicast |
ipv4-multicast]} originate-default
```

To enable or disable BGP default route origination and advertisement for a BGP peer group, use the following commands:

```
enable bgp {peer-group} <peer-group-name> {address-family [ipv4-unicast | ipv4-
multicast]} originate-default {policy <policy-name>}
disable bgp {peer-group} <peer-group-name> {address-family [ipv4-unicast | ipv4-
multicast]} originate-default
```

Example: Default Route Origination

The following example configures the originate default route feature for BGP neighbor *10.203.134.5* using policy *def_originate.pol*.

```
def_originate.pol

entry prefix_matching {
    if match any {
        nlri 192.168.3.0/24;
    } then {
        as-path "65001";
        permit;
    }
```

```
}

enable bgp neighbor 10.203.134.5 originate-default policy def_originate
```

With this configuration, a default route is originated and sent to neighbor 10.203.134.5 only if there is a BGP route in the local RIB which matches the statement `nlri 192.168.3.0/24`. If a matching route exists, the default route is sent to neighbor 10.203.134.5 with the `65001` as-path prepended. If this is an EBGP neighbor, then the local AS-Number is prepended *after* 65001.

If the route for the match statement `nlri 192.168.3.0/24` goes away and there is no other matching route in the BGP RIB, the default route origination feature becomes inactive and BGP withdraws the 0.0.0.0/0 default route from neighbor 10.203.134.5. When a matching route becomes available again in the local BGP RIB, the default route origination feature becomes active again and the default route 0.0.0.0/0 is advertised to neighbor 10.203.134.5.

Commands for Default Route Origination and Advertisement

The following commands have been added or modified to support this feature:

- disable bgp neighbor originate-default on page 13
- disable bgp peer-group originate-default on page 14
- enable bgp neighbor originate-default on page 15
- enable bgp peer-group originate-default on page 17
- show bgp neighbor <remoteaddr>
- show bgp neighbor detail

disable bgp neighbor originate-default

```
disable bgp [{neighbor} <remoteaddr> | neighbor all] {address-family [ipv4-
unicast | ipv4-multicast]} originate-default
```

Description

Removes a default route to a single BGP neighbor or to all BGP neighbors.

Syntax Description

{neighbor} <remoteaddr>	Specifies the IP address of a BGP neighbor for which the default route is removed.
neighbor all	Specifies that default routes are to be removed for all BGP neighbors.
ipv4-unicast	Specifies that the removed default routes apply to IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Specifies that the removed default routes apply to IPv4 multicast routes.

Default

Disabled. BGP does not automatically originate and advertise default routes to BGP neighbors.

Usage Guidelines

This command can be successfully executed at any time, irrespective of whether local BGP or the remote BGP peer is enabled or disabled.

Example

The following command removes default routes for IPv4 unicast traffic for all BGP peer nodes:

```
disable bgp neighbor all originate-default
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

disable bgp peer-group originate-default

```
disable bgp {peer-group} <peer-group-name> {address-family [ipv4-unicast |
ipv4-multicast]} originate-default
```

Description

Removes default routes to all BGP neighbors in the specified peer group.

Syntax Description

{peer-group} <peer-group-name>	Specifies the BGP peer group for which the default routes are removed.
ipv4-unicast	Specifies that the default routes apply to IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Specifies that the default routes apply to IPv4 multicast routes.

Default

Disabled. BGP does not automatically originate and advertise default routes to BGP neighbors.

Usage Guidelines

This command can be successfully executed at any time, irrespective of whether local BGP or the remote BGP peers are enabled or disabled.

Example

The following command removes default routes for IPv4 unicast traffic for all nodes in the *test* BGP peer group:

```
disable bgp peer-group test originate-default
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

enable bgp neighbor originate-default

```
enable bgp [{neighbor} <remoteaddr> | neighbor all] {address-family [ipv4-
unicast | ipv4-multicast]} originate-default {policy <policy-name>}
```

Description

Enables the origination and advertisement of a default route to a single BGP neighbor or to all BGP neighbors.

Syntax Description

{neighbor} <remoteaddr>	Specifies the IP address of a BGP neighbor for which the default route is originated and advertised.
neighbor all	Specifies that default routes are to be originated and advertised for all BGP neighbors.
ipv4-unicast	Specifies that the default routes apply to IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Specifies that the default routes apply to IPv4 multicast routes.
<policy-name>	Specifies a policy to be applied to the default route origination.

Default

Disabled. BGP does not automatically originate and advertise default routes to BGP neighbors.

Usage Guidelines

This command can be successfully executed at any time, irrespective of whether local BGP or the remote BGP peer is enabled or disabled. The default route or routes are created regardless of whether or not there are matching entries in the IP route table.

When a BGP neighbor is added to a peer group, it does not inherit the default route origination configuration from the peer group. Also, default route origination for a neighbor and the associated peer group can be different.

If a policy is configured and specified in the command, a default route can be originated only if there is a route in the local BGP RIB that matches the policy's match rules. The default route's attribute can be modified using the same policy file by including statements in the *set* block of the policy.

Example

The following command enables the origination and advertisement of default routes for IPv4 unicast traffic for all BGP peer nodes:

```
enable bgp neighbor all originate-default
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

enable bgp peer-group originate-default

```
enable bgp {peer-group} <peer-group-name> {address-family [ipv4-unicast |
ipv4-multicast]} originate-default {policy <policy-name>}
```

Description

Enables the origination and advertisement of default routes to all BGP neighbors in the specified peer group.

Syntax Description

{peer-group} <peer-group-name>	Specifies the BGP peer group for which the default routes are originated and advertised.
ipv4-unicast	Specifies that the default routes apply to IPv4 unicast routes. If you do not specify an address family, the command applies to IPv4 unicast routes.
ipv4-multicast	Specifies that the default routes apply to IPv4 multicast routes.
<policy-name>	Specifies a policy to be applied to the default routes during origination.

Default

Disabled. BGP does not automatically originate and advertise default routes to BGP neighbors.

Usage Guidelines

This command can be successfully executed at any time, irrespective of whether local BGP or the remote BGP peers are enabled or disabled. The default routes are created regardless of whether or not there are matching entries in the IGP route table.

When a BGP neighbor is added to a peer group, it does not inherit the default route origination configuration from the peer group. Also, default route origination for a neighbor and the associated peer group can be different.

If a policy is configured and specified in the command, a default route can be originated only if there is a route in the local BGP RIB that matches the policy's match rules. The default route's attribute can be modified using the same policy file by including statements in the *set* block of the policy.

Example

The following command enables the origination and advertisement of default routes for IPv4 unicast traffic for all nodes in the *test* BGP peer group:

```
enable bgp peer-group test originate-default
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

BGP ECMP

The BGP Equal Cost Multi-path (ECMP) feature supports load sharing by creating a multipath to a destination. This multipath contains multiple routes that are determined to have an equal cost because the following parameters are the same for each route:

- Weight
- Local preference (for IBGP multipaths)
- AS path (entire attribute, not just the length)
- Origin code
- Multi Exit Discriminator (MED)
- IGP distance to the next hop
- Source session (EBGP or IBGP)

NOTE

ECMP does not install an additional path if the next hop is the same as that of the best path. All paths within a multipath must have a unique next hop value.

BGP ECMP does not affect the best path selection. For example, the router continues to designate one of the paths as the best path and advertise this best path to its neighbors. EBGP paths are preferred to IBGP paths.

The BGP ECMP feature allows you to define the maximum number of equal cost paths (up to eight) in a multipath. A multipath for an IBGP destination is called an IBGP multipath, and the multipath for an EBGP destination is called an EBGP multipath.

If there are more equal cost paths for a destination than the configured maximum, the BGP identifier for the advertising BGP speaker is used to establish a path priority. The lower BGP identifier values have priority over the higher values. For example, if the configuration supports 4 paths in a multipath, only the four paths with the lowest BGP identifier values become part of the multipath.

To enable or disable BGP ECMP, enter the following command:

```
configure bgp maximum-paths <max-paths>
```

The `max-paths` setting applies to BGP on the current VR. Specify more than 1 path to enable BGP ECMP and define the maximum number of paths for IBGP and EBGP multipaths. Specify 1 path to disable ECMP. To display BGP ECMP configuration information, use the `show bgp` command.

The following commands have been added or modified to support this feature:

- configure bgp maximum-paths on page 20
- show bgp on page 21
- show bgp routes on page 23

configure bgp maximum-paths

```
configure bgp maximum-paths <max-paths>
```

Description

Enables or disables the BGP ECMP feature and specifies the maximum number of paths supported on the current VR.

Syntax Description

max-paths	Specifies the maximum number of paths. The range is 1 to 8. The value 1 disables BGP ECMP. A value greater than 1 enables BGP ECMP and specifies the maximum number of paths.

Default

One. BGP ECMP is disabled.

Usage Guidelines

This command triggers the BGP decision process, causing BGP to re-install the entire BGP routing table into the IP forwarding table. This activity requires a significant amount of switch processor resources, so we recommend that you enable or disable the BGP ECMP feature before enabling the BGP protocol globally on a VR. Run the `enable iproute sharing` command to ensure that BGP ECMP routes are programmed in the hardware.

Example

The following command enables BGP ECMP and sets the maximum number of paths to *4*:

```
configure bgp maximum-paths 4
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

show bgp

```
show bgp
```

Description

Displays BGP configuration information.

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

None.

Example

The following command displays BGP configuration information:

```
# show bgp

Enabled             : Yes               OperStatus          : Up
RouterId            : 10.203.134.73     As                  : 100
LocalPref           : 100               MED                 : None
Always-Compare-MED  : Disabled          Aggregation         : Disabled
Route Reflector     : No                RR ClusterId        : 0
IGP Synchronization : Disabled          New Community Format: Disabled
Routes from EBGP    : 2                 Routes from IBGP    : 0
Routes redistributed: 0                 Out Updates queued  : 0
Fast Ext Fallover   : Disabled          MPLS LSP as Next-Hop: No
ConfedId            : 0                 Maximum ECMP Paths  : 5
Confed Peers        :
Networks            : 0
Aggregate Networks  : 0
Redistribute:
  ipv4       Admin     Operational  Shutdown  Policy
  unicast    Status    Status       Priority
  ------------------------------------------------------
  Direct     Disabled  Down         2048      None
  Static     Disabled  Down         2048      None
  RIP        Disabled  Down         2048      None
  OSPFIntra  Disabled  Down         2048      None
  OSPFInter  Disabled  Down         2048      None
  OSPFExt1   Disabled  Down         2048      None
  OSPFExt2   Disabled  Down         2048      None
  ISISL1     Disabled  Down         2048      None
```

```
  ISISL2      Disabled  Down          2048      None
  ISISL1Ext   Disabled  Down          2048      None
  ISISL2Ext   Disabled  Down          2048      None

  ipv4        Admin     Operational   Shutdown  Policy
  multicast   Status    Status        Priority
  ------------------------------------------------------
  Direct      Disabled  Down          2048      None
  Static      Disabled  Down          2048      None
  RIP         Disabled  Down          2048      None
  OSPFIntra   Disabled  Down          2048      None
  OSPFInter   Disabled  Down          2048      None
  OSPFExt1    Disabled  Down          2048      None
  OSPFExt2    Disabled  Down          2048      None
  ISISL1      Disabled  Down          2048      None
  ISISL2      Disabled  Down          2048      None
  ISISL1Ext   Disabled  Down          2048      None
  ISISL2Ext   Disabled  Down          2048      None
Advertise Inactive Routes:
  ipv4-unicast   : Disabled
  ipv4-multicast : Disabled
```

History

This command was first available in ExtremeXOS 10.1.

This command required a specific license in ExtremeXOS 11.1.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

show bgp routes

```
show bgp routes {address-family [ipv4-unicast | ipv4-multicast]} {detail}
[all | as-path <path-expression> | community [no-advertise | no-export |
no-export-subconfed | number <community_num> | <AS_Num>:<Num>] | network
[any / <netMaskLen> | <networkPrefixFilter>] {exact}]
```

Description

Displays the BGP route information base (RIB).

Syntax Description

address-family	The address family. BGP supports two address families: IPv4 Unicast and IPv4 Multicast.
all	Specifies all routes.
no-advertise	Specifies the no-advertise community attribute.
no-export	Specifies the no-export community attribute.
no-export-subconfed	Specifies the no-export-subconfed community attribute.
community_num	Specifies a community number.
AS_Num	Specifies an autonomous system ID (0-65535).
Num	Specifies the BGP community number.
any	Specifies all routes with a given or larger mask length.
netMaskLen	Specifies a subnet mask length (number of bits).
networkPrefixFilter	Specifies an IP address and netmask.
exact	Specifies an exact match with the IP address and subnet mask.

Default

If no address family is specified, IPv4 unicast is the default.

Usage Guidelines

The option `network any / <netMaskLen>` displays all BGP routes whose mask length is equal to or greater than `<maskLength>`, irrespective of their network address.

The option `network any / <netMaskLen> exact` displays all BGP routes whose mask length is exactly equal to `<maskLength>`, irrespective of their network address.

Example

The following command displays detailed information about all BGP routes:

```
# # show bgp  routes all

Feasible Routes
---------------
   Destination        Peer            Next-Hop        LPref Weight MED   AS-Path
*>i3.0.0.0/8          80.0.0.69       80.0.0.1        100   1            65070 14490
10911 1239
 m>i3.0.0.0/8          90.0.0.69       90.0.0.1        100   1            65070 14490
10911 1239
 m>i3.0.0.0/8          60.0.0.69       60.0.0.1        100   1            65070 14490
10911 1239
*>i4.17.226.0/24      80.0.0.69       80.0.0.1        100   1            65070 14490
10911 3561
m >i4.17.226.0/24      90.0.0.69       90.0.0.1        100   1            65070 14490
10911 3561
```

The following command displays detailed information about all BGP routes:

```
# show bgp routes detail all

Feasible Routes
---------------
Route: 3.0.0.0/8,  Peer 80.0.0.69,  Multipath, BEST, Active
Origin IGP, Next-Hop 80.0.0.1, LPref 100
Weight 1,
AS-Path: 65070 14490 10911 1239 80

Route: 3.0.0.0/8,  Peer 90.0.0.69,  Multipath, Active
Origin IGP, Next-Hop 90.0.0.1, LPref 100
Weight 1,
AS-Path: 65070 14490 10911 1239 80

Route: 3.0.0.0/8,  Peer 60.0.0.69,  Multipath, Active
Origin IGP, Next-Hop 60.0.0.1, LPref 100
Weight 1,
AS-Path: 65070 14490 10911 1239 80

Route: 4.17.226.0/24,  Peer 80.0.0.69,  Multipath, BEST, Active
Origin IGP, Next-Hop 80.0.0.1, LPref 100
Weight 1,
AS-Path: 65070 14490 10911 3561 11853 6496 6496 6496 6496

Route: 4.17.226.0/24,  Peer 90.0.0.69,  Multipath, Active
Origin IGP, Next-Hop 90.0.0.1, LPref 100
Weight 1,
AS-Path: 65070 14490 10911 3561 11853 6496 6496 6496 6496
```

History

This command was first available in ExtremeXOS 10.1.

The `any / <netMaskLen>` options were added in ExtremeXOS 11.0.

This command required a specific license in ExtremeXOS 11.1.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

Support for Overlapping Aggregate Routes

BGP now supports overlapping routes. The following command description has been updated for this feature:

- configure bgp add aggregate-address on page 26

configure bgp add aggregate-address

```
configure bgp add aggregate-address {address-family [ipv4-unicast |
ipv4-multicast]} <ipaddress> {as-match | as-set} {summary-only}
{advertise-policy <policy>} {attribute-policy <policy>}
```

Description

Configures a BGP aggregate route.

Syntax Description

address-family	The address family. BGP supports two address families: IPv4 unicast and IPv4 multicast.
ipaddress	Specifies an IP network address and mask length.
as-match	Generates autonomous system sequence path information (order of AS numbers in AS_PATH is preserved).
as-set	Generates autonomous system set path information (order of AS numbers in AS_PATH is not preserved).
summary-only	Specifies to send only aggregated routes to the neighbors.
advertise-policy	Specifies the policy used to select routes for this aggregated route.
attribute-policy	Specifies the policy used to set the attributes of the aggregated route.

Default

If no address family is specified, IPv4 unicast is the default.

Usage Guidelines

Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

Before you can create an aggregate route, you must enable BGP aggregation using the following command:

```
enable bgp aggregation
```

BGP supports overlapping routes. For example, you can configure both of the following aggregate addresses:

- 192.0.0.0/8
- 192.168.0.0/16

After you create an aggregate route, the aggregate route remains inactive until BGP receives a route with an IP address and mask that conforms to an aggregate route. When a conforming route is received, the aggregate route becomes active and is advertised to BGP neighbors. If the `summary-only` option is specified, only the aggregate route becomes active and is advertised. If the `summary-only` option is omitted, any conforming aggregate routes and the received route are advertised to BGP neighbors.

Example

The following command configures a BGP aggregate route:

```
configure bgp add aggregate-address 192.1.1.4/30
```

History

This command was first available in ExtremeXOS 10.1.

This command required a specific license in ExtremeXOS 11.1.

Support for overlapping aggregate addresses was added in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

Blackhole Route Redistribution

BGP now supports the redistribution of blackhole routes. The following commands have been updated to support this feature:

- disable bgp export on page 28
- enable bgp export on page 30

disable bgp export

```
disable bgp export [blackhole | direct | isis | isis-level-1 | isis-level-
1-external | isis-level-2 | isis-level-2-external | ospf | ospf-extern1 |
ospf-extern2 | ospf-inter | ospf-intra | rip | static {address-family
[{ipv4-unicast |ipv4-multicast]}
```

Description

Disables BGP from exporting routes from other protocols to BGP peers.

Syntax Description

blackhole	Specifies blackhole routes.
direct	Specifies direct routes.
isis	Specifies ISIS routes.
isis-level-1	Specifies ISIS-level-1 routes.
isis-level-1-external	Specifies ISIS-level-1 external routes.
isis-level-2	Specifies ISIS-level-2 routes.
isis-level-2-external	Specifies ISIS-level-2 external routes.
ospf	Specifies OSPF routes.
ospf-extern1	Specifies OSPF-extern1 routes.
ospf-extern2	Specifies OSPF-extern2 routes.
ospf-inter	Specifies OSPF-inter routes.
ospf-intra	Specifies OSPF-intra routes.
rip	Specifies RIP routes.
static	Specifies static routes.
address-family	The address family to which the IGP routes is exported. BGP supports two address families: IPv4 Unicast and IPv4 Multicast.

Default

Disabled.

If no address family is specified, IPv4 unicast is the default.

Usage Guidelines

The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use policies to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. Policies can also be used to filter out exported routes.

Using the export command to redistribute routes complements the redistribution of routes using the configure bgp add network command. The configure bgp add network command adds the route to BGP only if the route is present in the routing table. The enable bgp export command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.

Example

The following command disables BGP from exporting routes from the OSPF protocol to BGP peers:

```
disable bgp export ospf
```

History

This command was first available in ExtremeXOS 10.1.

This command required a specific license in ExtremeXOS 11.1.

The `blackhole` option was added in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

enable bgp export

```
enable bgp export [blackhole | direct | isis | isis-level-1 | isis-level-1-
external | isis-level-2 | isis-level-2-external | ospf | ospf-extern1 |
ospf-extern2 | ospf-inter | ospf-intra | rip | static {address-family
[{ipv4-unicast |ipv4-multicast]} {export-policy <policy-name>}
```

Description

Enables BGP to export routes from other protocols to BGP peers.

Syntax Description

blackhole	Specifies blackhole routes.
direct	Specifies direct routes.
isis	Specifies ISIS routes.
isis-level-1	Specifies ISIS-level-1 routes.
isis-level-1-external	Specifies ISIS-level-1 external routes.
isis-level-2	Specifies ISIS-level-2 routes.
isis-level-2-external	Specifies ISIS-level-2 external routes.
ospf	Specifies OSPF routes.
ospf-extern1	Specifies OSPF-extern1 routes.
ospf-extern2	Specifies OSPF-extern2 routes.
ospf-inter	Specifies OSPF-inter routes.
ospf-intra	Specifies OSPF-intra routes.
rip	Specifies RIP routes.
static	Specifies static routes.
address-family	The address family to which the IGP routes are exported. BGP supports two address families: IPv4 Unicast and IPv4 Multicast.
policy-name	Name of policy to be associated with network export. Policy can filter and/or change the route parameters.

Default

Disabled.

If no address family is specified, IPv4 unicast is the default.

Usage Guidelines

The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then, you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use a policy to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. A policy can also be used to filter out exported routes.

Using the export command to redistribute routes complements the redistribution of routes using the configure bgp add network command. The configure bgp add network command adds the route to BGP only if the route is present in the routing table. The enable bgp export command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.

Example

The following command enables BGP to export routes from the OSPF protocol to BGP peers:

```
enable bgp export ospf
```

History

This command was first available in ExtremeXOS 10.1.

This command required a specific license in ExtremeXOS 11.1.

The `blackhole` option was added in ExtremeXOS 12.1.3.

Platform Availability

This command is available on platforms with the appropriate license. For complete information about software licensing, including how to obtain and upgrade your license and what licenses are appropriate for this feature, see the *ExtremeXOS Concepts Guide*, Appendix A, "ExtremeXOS Software Licenses."

Flow Control—Summit Family of Switches and BlackDiamond 8800 Series Switches Only

With autonegotiation enabled, the Summit® family of switches and the BlackDiamond® 8800 series switches advertise the ability to support pause frames. This includes receiving, reacting to (stopping transmission), and transmitting pause frames. However, the switch does not actually transmit pause frames unless it is configured to do so, as described below.

IEEE 802.3x flow control provides the ability to configure different modes in the default behaviors. Ports can be configured to transmit pause frames when congestion is detected, and the behavior of reacting to received pause frames can be disabled.

TX

You can configure ports to transmit link-layer pause frames upon detecting congestion. The goal of IEEE 802.3x is to backpressure the ultimate traffic source to eliminate or significantly reduce the amount of traffic loss through the network. This is also called lossless switching mode.

The following limitations apply to the TX flow control feature:

- Flow control is applied on an ingress port basis which means that a single stream ingressing a port and destined to a congested port can stop the transmission of other data streams ingressing the same port which are destined to other ports.
- High volume packets destined to the CPU can cause flow control to trigger. This includes protocol packets such as, EDP, EAPS, VRRP, and OSPF.
- When flow control is applied to the fabric ports, there can be a performance limitation. For example, a single 1G port being congested could backpressure a high-speed fabric port and reduce its effective throughput significantly.

To configure a port to allow the transmission of IEEE 802.3x pause frames, use the following command:

```
enable flow-control tx-pause ports
```

NOTE

To enable TX flow-control, RX flow-control must first be enabled. If you attempt to enable TX flow-control with RX flow-control disabled, an error message is displayed.

To configure a port to return to the default behavior of not transmitting pause frames, use the following command:

```
disable flow-control tx-pause ports
```

RX

You can configure the switch to disable the default behavior of responding to received pause frames. Disabling rx-pause processing avoids dropping packets in the switch and allows for better overall network performance in some scenarios where protocols such as TCP handle the retransmission of dropped packets by the remote partner.

To configure a port to disable the processing of IEEE 802.3x pause frames, use the following command:

```
disable flow-control rx-pause ports
```

NOTE

To disable RX flow-control, TX flow-control must first be disabled. If you attempt to disable RX flow-control with TX flow-control enabled, an error message is displayed.

To configure a port to return to the default behavior of enabling the processing of pause frames, use the following command:

```
enable flow-control rx-pause ports
```

disable flow-control rx-pause ports

```
disable flow-control rx-pause ports [<port_list> | all]
```

Description

Disables the processing of received pause flow control messages.

Syntax Description

port_list	Specifies one or more ports or slots and ports.

Default

Enabled

Usage Guidelines

With autonegotiation enabled, the Summit family of switches and the BlackDiamond® 8800 series switches advertise the ability to support pause frames. This includes receiving and reacting to (stopping transmission) pause frames.

Use this command to disable the processing of IEEE 802.3x pause flow control messages received from the remote partner. Disabling rx-pause processing avoids dropping packets in the switch and allows for better overall network performance in some scenarios where protocols such as TCP handle the retransmission of dropped packets by the remote partner.

To disable RX flow-control, TX flow-control must first be disabled. Refer to the `disable flow-control tx-pause ports` command. If you attempt to disable RX flow-control with TX flow-control enabled, an error message is displayed.

Example

The following command disables the rx flow-control feature on ports 5 through 7 on a Summit® switch:

```
disable flow-control rx-pause ports 5-7
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on the BlackDiamond 8800 series modules and the Summit family of switches.

disable flow-control tx-pause ports

```
disable flow-control tx-pause ports [<port_list> | all]
```

Description

Disables the transmission of pause frames.

Syntax Description

port_list	Specifies one or more ports or slots and ports.

Default

Disabled

Usage Guidelines

Use this command to stop the transmission of flow control pause frames and revert to the default.

Example

The following command disables the tx flow-control feature on ports 5 through 7 on a Summit switch:

```
disable flow-control tx-pause ports 5-7
```

History

This command was first available in ExtremeXOS 12.1.3

Platform Availability

This command is available on the BlackDiamond 8800 series modules and the Summit family of switches.

enable flow-control rx-pause ports

```
enable flow-control rx-pause ports [<port_list> | all]
```

Description

Enables the switch to process received pause frames.

Syntax Description

port_list	Specifies one or more ports or slots and ports.

Default

Enabled

Usage Guidelines

Use this command to configure the switch to return to the default behavior of processing received pause frames.

Example

The following command enables the tx flow-control feature on ports 5 through 7 on a Summit switch:

```
enable flow-control rx-pause ports 5-7
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on the BlackDiamond 8800 series modules and the Summit family of switches.

enable flow-control tx-pause ports

```
enable flow-control tx-pause ports [<port_list> | all]
```

Description

Enables the switch to transmit pause frames.

Syntax Description

port_list	Specifies one or more ports or slots and ports.

Default

Disabled

Usage Guidelines

With autonegotiation enabled, the Summit family of switches and the BlackDiamond 8800 series switches advertise the ability to support pause frames. This includes receiving, reacting to (stopping transmission), and transmitting pause frames. However, the switch does not actually transmit pause frames unless it is configured to do so.

IEEE 802.3x flow control provides the ability to configure different modes in the default behaviors. Use this command to configure the switch to transmit link-layer pause frames when congestion is detected.

To enable TX flow-control, RX flow-control must first be enabled. Refer to the `enable flow-control rx-pause ports` command. If you attempt to enable TX flow-control with RX flow-control disabled, an error message is displayed.

Example

The following command enables the tx flow-control feature on ports 5 through 7 on a Summit switch:

```
enable flow-control tx-pause ports 5-7
```

History

This command was first available in ExtremeXOS 12.1.2 patch 4

Platform Availability

This command is available on the BlackDiamond 8800 series modules and the Summit family of switches.

show ports information

```
show ports {mgmt | <port_list>} information {detail}
```

Description

Displays detailed system-related information.

Syntax Description

mgmt	Specifies the management port.
port_list	Specifies one or more ports of slots and ports.
detail	Specifies detailed port information.

Default

N/A.

Usage Guidelines

This command displays information, including the following:

- Port number
- Port configuration
  - Virtual router
  - Type of port
  - Admin state
  - Link state and speed
  - Link counter
  - VLAN configuration
  - STP configuration
  - Trunking, or load sharing
  - EDP
  - ELSM (disabled; or if enabled, the ELSM link state is shown as well)
  - Load balancing
  - Learning
  - Egress flooding
  - Jumbo frames
  - Link port up/down traps
  - QoS profiles
  - vMAN status
  - Smart Redundancy status
  - SRP status

- Additional platform-specific information
- LW XENPAK WAN PHY ports—BlackDiamond 10808 switch and Summit X450a series switch only
  - Framing
  - Clocking
  - Trace section
  - Trace path

If you do not specify a port number or range of ports, detailed system-related information is displayed for all ports. The data is displayed in a table format.

This status information may be useful for your technical support representative if you have a network problem.

The `detail` parameter is used to provided more specific port information. The data is called out with written explanations versus displayed in a table format.

NOTE

The keyword `detail` *displays slightly different information depending on the platform and configuration you are working with.*

The link filter counter displayed with the `detail` keyword is calculated at the middle layer on receiving an event. The link filter up indicates the number of link transitions from down to up at the middle layer filter.

Example

The following command displays port system-related information on a BlackDiamond 8810 switch:

```
X450a-48t.10 # show port 1 info
```

Following is sample output from this command:

```
Port      Flags           Link           Link Num Num  Num   Jumbo QOS     Load
                          State     ELSM UPS  STP VLAN Proto Size  profile Master
================================================================================
1         Ew------e--fMB- ready      -     0    0    1   1   9194  none
================================================================================
> indicates Port Display Name truncated past 8 characters
Flags : a - Load Sharing Algorithm address-based, D - Port Disabled,
        e - Extreme Discovery Protocol Enabled, E - Port Enabled,
        g - Egress TOS Enabled, j - Jumbo Frame Enabled,
        l - Load Sharing Enabled, m - MACLearning Enabled,
        n - Ingress TOS Enabled, o - Dot1p Replacement Enabled,
        P - Software redundant port(Primary),
        R - Software redundant port(Redundant),
        q - Background QOS Monitoring Enabled,
        s - diffserv Replacement Enabled,
        v - Vman Enabled, f - Unicast Flooding Enabled,
        M - Multicast Flooding Enabled, B - Broadcast Flooding Enabled
        L - Extreme Link State Monitoring Enabled
        w - MACLearning Disabled with Forwarding, b - Rx and Tx Flow Control Enabled,
x - Rx Flow Control Enabled. - - Rx and Tx Flow Control Disabled.
```

NOTE

The BlackDiamond 10808, 12800, and 20808 series switches have an additional flag: `p - Load Sharing Algorithm port-based.`

The following command displays detailed port system-related information on a BlackDiamond 8810 switch:

```
show port 1:1 info detail
```

Following is sample output from this command:

```
Port:   1:1
        Virtual-router: VR-Default
        Type:           UTP
        Random Early drop:      Unsupported
        Admin state:    Enabled with  auto-speed sensing  auto-duplex
        Link State:     Ready
        Link Counter: Up        0 time(s)


        VLAN cfg:
                Name: v1, Internal Tag = 4093, MAC-limit = No-limit, Virtual router:
VR-Default

        STP cfg:

        Protocol:
                Name: v1            Protocol: ANY      Match all protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Disabled
        Learning:       Disabled (forward-packets)
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Disabled
        Flow Control:   Tx-Pause: Enabled
        Link up/down SNMP trap filter setting:  Enabled
        Egress Port Rate:       No-limit
        Broadcast Rate:         No-limit
        Multicast Rate:         No-limit
        Unknown Dest Mac Rate:  No-limit
        QoS Profile:    None configured
        Ingress Rate Shaping :          Unsupported
        Ingress IPTOS Examination:      Disabled
        Ingress 802.1p Examination:     Enabled
        Ingress 802.1p Inner Exam:      Disabled
        Egress IPTOS Replacement:       Disabled
        Egress 802.1p Replacement:      Disabled
        NetLogin:                       Disabled
        NetLogin port mode:             Port based VLANs
        Smart redundancy:               Enabled
        Software redundant port:        Disabled
        auto-polarity:                  Enabled
```

BlackDiamond 8800 series switch, SummitStack™, and the Summit family of switches only. The following command displays more specific information for slot 3, port 1 on a BlackDiamond 8810 switch:

```
show ports 3:1 information detail
```

Following is sample output from this command:

```
Port:   3:1
        Virtual-router: VR-Default
        Type:           UTP
        Random Early drop:      Unsupported
        Admin state:    Enabled with  auto-speed sensing  (100M Advertised), auto-
duplex (half-duplex Advertised)
        ELSM Link State:   Up
        Link State:     Active, 1 Gbps, full-duplex
        Link Counter: Up        1 time(s)
        VLAN cfg:
                 Name: Default, Internal Tag = 1 (MAC-Based), MAC-limit = No-limit

        STP cfg:
                s0(disable), Tag=(none), Mode=802.1D, State=FORWARDING

        Protocol:
                 Name: Default      Protocol: ANY      Match all protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Enabled
        Learning:       Enabled
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Enabled, MTU= 9194
        Flow Control:   Rx-Pause: Enabled Tx-Pause: Disabled
        Link up/down SNMP trap filter setting:  Enabled
        Egress Port Rate:       128 Kbps, Max Burst Size: 200 Kb
        Broadcast Rate:         No-limit
        Multicast Rate:         No-limit
        Unknown Dest Mac Rate:  No-limit
        QoS Profile:    QP3 configured by user
        Ingress Rate Shaping :          Unsupported
        Ingress IPTOS Examination:      Disabled
        Ingress 802.1p Examination:     Enabled
        Ingress 802.1p Inner Exam:      Disabled
        Egress IPTOS Replacement:       Disabled
        Egress 802.1p Replacement:      Disabled
        NetLogin:                       Enabled
        NetLogin authentication mode:   MAC based
        NetLogin port mode:             MAC based VLANs
        Smart redundancy:               Enabled
        Software redundant port:        Disabled
        autopolarity:                   Enabled
```

BlackDiamond 10808, BlackDiamond 12800, and BlackDiamond 20808 series switches only. The following command displays more specific information for slot 1, port 1 on a BlackDiamond 10808 switch:

```
show ports 1:1 information detail
```

Following is sample output from this command:

```
Port:   1:1
        Virtual-router: VR-Default
        Type:           UTP
        Random Early drop:      Unsupported
        Admin state:    Enabled with  auto-speed sensing  (100M Advertised), auto-
duplex (half-duplex Advertised)
        Link State:     Active, 100Mbps, full-duplex
        Link Counter: Up        1 time(s)
        VLAN cfg:
                 Name: peggy, Internal Tag = 4094, MAC-limit = No-limit

        STP cfg:

        Protocol:
                 Name: peggy        Protocol: ANY      Match all protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Disabled
        Learning:       Enabled
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Disabled
        Link up/down SNMP trap filter setting:  Enabled
        QoS Profile:    None configured
        Aggregate Queue:
                QP0  MinBw =          0% PR    =        100K  Pri = 8
        Queue:
                QP1  MinBw =          0% MaxBw =        100%  Pri = 1
                QP2  MinBw =          0% MaxBw =        100%  Pri = 2
                QP3  MinBw =          0% MaxBw =        100%  Pri = 3
                QP4  MinBw =          0% MaxBw =        100%  Pri = 4
                QP5  MinBw =          0% MaxBw =        100%  Pri = 5
                QP6  MinBw =          0% MaxBw =        100%  Pri = 6
                QP7  MinBw =          0% MaxBw =        100%  Pri = 7
                QP8  MinBw =          0% MaxBw =        100%  Pri = 8
        Ingress Rate Shaping :          support IQP1-2
                IQP1 MinBw =          0% MaxBw =        100%  Pri = 1
                IQP2 MinBw =          0% MaxBw =        100%  Pri = 2
        Ingress IPTOS Examination:      Disabled
        Egress IPTOS Replacement:       Disabled
        Egress 802.1p Replacement:      Disabled
        NetLogIn:                       Disabled
        Smart redundancy:               Enabled
        Software redundant port:        Enabled
          Primary:                      1:1
          Redundant:                    1:2
          Redundant link configuration: Off
        autopolarity:                   Enabled
```

NOTE

On the BlackDiamond 10808 switch, the screen displays both ingress and egress QoS settings. The 10Gbps ports have 8 ingress queues, and the 1 Gbps ports have 2 ingress queues.(Refer to the ExtremeXOS Concepts Guide *for more information on ingress queues, or bi-directional rate shaping.) The BlackDiamond 12800 series switch does not support ingress QoS settings.*

BlackDiamond 12800 R-series switch only. The following command displays more specific information for slot 2, port 1 on a BlackDiamond 12800 R-series switch:

```
show ports 2:1 information detail
```

Following is sample output from this command:

```
Port:   2:1
        Virtual-router: VR-Default
        Type:           NONE
        Random Early drop:      Unsupported
        Admin state:    Enabled with  10G full-duplex
        Link State:     Ready
        Link Counter: Up        0 time(s)
        VLAN cfg:
                 Name: Default, Internal Tag = 1, MAC-limit = No-limit, Virtual ro
uter: VR-Default

        STP cfg:
                s0(disable), Tag=(none), Mode=802.1D, State=FORWARDING

        Protocol:
                 Name: Default      Protocol: ANY      Match all protocols.
        Trunking:       Load sharing is not enabled.
        EDP:            Enabled
        ELSM:           Disabled
        Learning:       Enabled
        Unicast Flooding:       Enabled
        Multicast Flooding:     Enabled
        Broadcast Flooding:     Enabled
        Jumbo:          Disabled
        High Priority COS: 7
        Packet Length Adjustment: 0 bytes
        QoS Profile:    None configured
        Aggregate Queue:
                QP0  MinBw =          0% MaxBw =        100%  Pri = 8
        Queue:
                QP1  MinBw =          0% MaxBw =        100%  Pri = 1
                QP2  MinBw =          0% MaxBw =        100%  Pri = 2
                QP3  MinBw =          0% MaxBw =        100%  Pri = 3
                QP4  MinBw =          0% MaxBw =        100%  Pri = 4
                QP5  MinBw =          0% MaxBw =        100%  Pri = 5
                QP6  MinBw =          0% MaxBw =        100%  Pri = 6
                QP7  MinBw =          0% MaxBw =        100%  Pri = 7
                QP8  MinBw =          0% MaxBw =        100%  Pri = 8
        Ingress Rate Shaping :          Unsupported
        Ingress IPTOS Examination:      Disabled
        Egress IPTOS Replacement:       Disabled
        Egress 802.1p Replacement:      Disabled
```

```
        NetLogin:                       Disabled
        NetLogin port mode:             Port based VLANs
        Smart redundancy:               Enabled
        Software redundant port:        Disabled
        Preferred medium:               Fiber
```

NOTE

On the GM-20XT and GM-20XTR modules for the BlackDiamond 12800 series switch and 12800 R-series switches, you can use each port as either copper or fiber; `preferred medium` *displays which medium the specified port is using.*

BlackDiamond 10808 and 20808 switches and Summit X450a and X650 series switches (including SummitStack) with LW XENPAK ports only. The following command displays more specific information for the WAN PHY port on the LW XENPAK in port 1 of the Summit X450a -24t switch:

```
Port:   1
        Framing: SONET
        Clocking: Line
        LoopBack: Off
        Trace Section: alpha4
        Trace Path:    delta6
```

History

This command was first available in ExtremeXOS 10.1.

Information on ingress rate shaping was added in ExtremeXOS 11.0.

NetLogIn, Smart Redundancy, and rate limiting were added in ExtremeXOS 11.1.

Information on unicast, multicast, and broadcast flooding; the `Port not present` parameter; and autopolarity status were added in ExtremeXOS 11.2.

The `netlogin` parameters were added in ExtremeXOS 11.3.

The BlackDiamond 12800 R-series specific parameters were added in ExtremeXOS 11.4.

Information on WAN PHY ports on the LW XENPAK modules on the BlackDiamond 10808 switch and the Summit X450a series switches was added in ExtremeXOS 11.6.

The output command was modified in ExtremeXOS 12.1 so that when learning is disabled with the `disabled learning port` command, a new w flag appears in the output.

TX Flow control was added in ExtremeXOS 12.1.2 patch 4 for the BlackDiamond 8800 series modules and the Summit family of switches. RX Flow control was added in ExtremeXOS 12.1.3.

Platform Availability

This command is available on all platforms. (Information on WAN PHY ports on the LW XENPAK modules is available only on the BlackDiamond 10808 switch, BlackDiamond 12800 series switches, BlackDiamond 20808 series switches, and the Summit X450a and X650 series switches, whether or not included in a SummitStack.

STP and Network Login

Spanning Tree Protocol (STP) and Network Login work on the edge port with safeguard only. If a port has netlogin enabled but does not have STP safeguard enabled, the STP domain cannot be enabled. This feature works with spanning tree operational mode dot1w and MSTP.

Limitation: This feature does not support network login in Campus mode.

STP works in three port modes:

- Extreme Multiple Instance Spanning Tree Protocol (EMISTP) mode

  EMISTP mode is proprietary to Extreme Networks® and is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs. EMISTP adds significant flexibility to STP network design. BPDUs are sent with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field.

  This encapsulation mode supports the following STPD modes of operation: 802.1D and 802.1w.

- Per VLAN Spanning Tree (PVST+) mode

  This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

  This encapsulation mode supports the following STPD modes of operation: 802.1D and 802.1w.

- dot1d

  This mode is reserved for backward compatibility with previous STP versions. BPDUs are sent running in 802.1D mode.

  This encapsulation mode supports the following STPD modes of operation: 802.1D, 802.1w, and MSTP.

In PVST+ and EMISTP modes, carrier VLAN restrictions are imposed (see the *ExtremeXOS Concepts Guide* for more information about carrier VLANs). If all ports are in dot1d mode, there are no carrier VLAN restrictions.

NOTE

STP domains should be enabled after completing safeguard configurations. Each netlogin port should be enabled with safeguard. If you add a new netlogin port to an already enabled STP domain, disable the spanning tree domain and then enable it again.

Refer to the following configurations when running STP and netlogin on an edge port.

```
# Module vlan configuration.
#
configure vlan default delete ports 1-50
create vlan "net-log"
create vlan "v10"
configure vlan v10 tag 10
configure vlan v10 add ports 1-48 untagged
configure vlan v10 ipaddress 192.168.10.254 255.255.255.0

# Module aaa configuration.
#
create netlogin local-user "0002b3ed4244" encrypted "9xSkxd$3gF45Qa9vhdnzdWPFr7Vs0"
create netlogin local-user "000f1ffed625" encrypted "P1G8rd$ADwsxR2U9PMqLLOfL02U4/"
create netlogin local-user "001676dd3ba1" encrypted "53inVd$l4u9aDnRAgDMbXnBNapvk1"
```

```
# Module netLogin configuration.
#
configure netlogin vlan net-log
enable netlogin mac
enable netlogin ports 1-10 mac
configure netlogin ports 1 mode port-based-vlans
configure netlogin ports 1 no-restart
configure netlogin ports 2 mode port-based-vlans
configure netlogin ports 2 no-restart

configure netlogin add mac-list 00:02:b3:ed:42:44 48 encrypted "canrli"
configure netlogin add mac-list 00:0f:1f:fe:d6:25 48 encrypted "canrli"
configure netlogin add mac-list 00:16:76:dd:3b:a1 48 encrypted "canrli"

# Module stp configuration.
#
create stpd s10
configure stpd s10 mode dot1w
configure stpd s10 add vlan v10 ports 1 dot1d
configure stpd s10 add vlan v10 ports 2 dot1d
configure stpd s10 add vlan v10 ports 47 dot1d
configure stpd s10 add vlan v10 ports 48 dot1d

configure stpd s10 ports mode dot1d 1
configure stpd s10 ports cost auto 1
configure stpd s10 ports port-priority 128 1
configure stpd s10 ports link-type edge 1
configure stpd s10 ports edge-safeguard enable 1
enable stpd s10 ports 1
configure stpd s10 ports mode dot1d 2
configure stpd s10 ports cost auto 2
configure stpd s10 ports port-priority 128 2
configure stpd s10 ports link-type edge 2
configure stpd s10 ports edge-safeguard enable 2
enable stpd s10 ports 2
configure stpd s10 ports mode dot1d 47
configure stpd s10 ports cost auto 47
configure stpd s10 ports port-priority 128 47
configure stpd s10 ports link-type point-to-point 47
configure stpd s10 ports edge-safeguard disable 47
enable stpd s10 ports 47
configure stpd s10 ports mode dot1d 48
configure stpd s10 ports cost auto 48
configure stpd s10 ports port-priority 128 48
configure stpd s10 ports link-type point-to-point 48
configure stpd s10 ports edge-safeguard disable 48
enable stpd s10 ports 48
enable stpd s10
```

EXTREME STP NOTIFICATIONS MIB

This MIB defines the following Extreme-specific STP Notifications trap generated by Extreme Networks devices. The following MIB is defined in extremeStp.my.

Trap	Comments
extremeStpEdgePortLoopDetected	A loop has been detected on the netlogin edge safeguard port and the port will be disabled.

Health Check Link Aggregation

The following sections discuss the Health Check Link Aggregation feature.

Health Check Link Aggregation

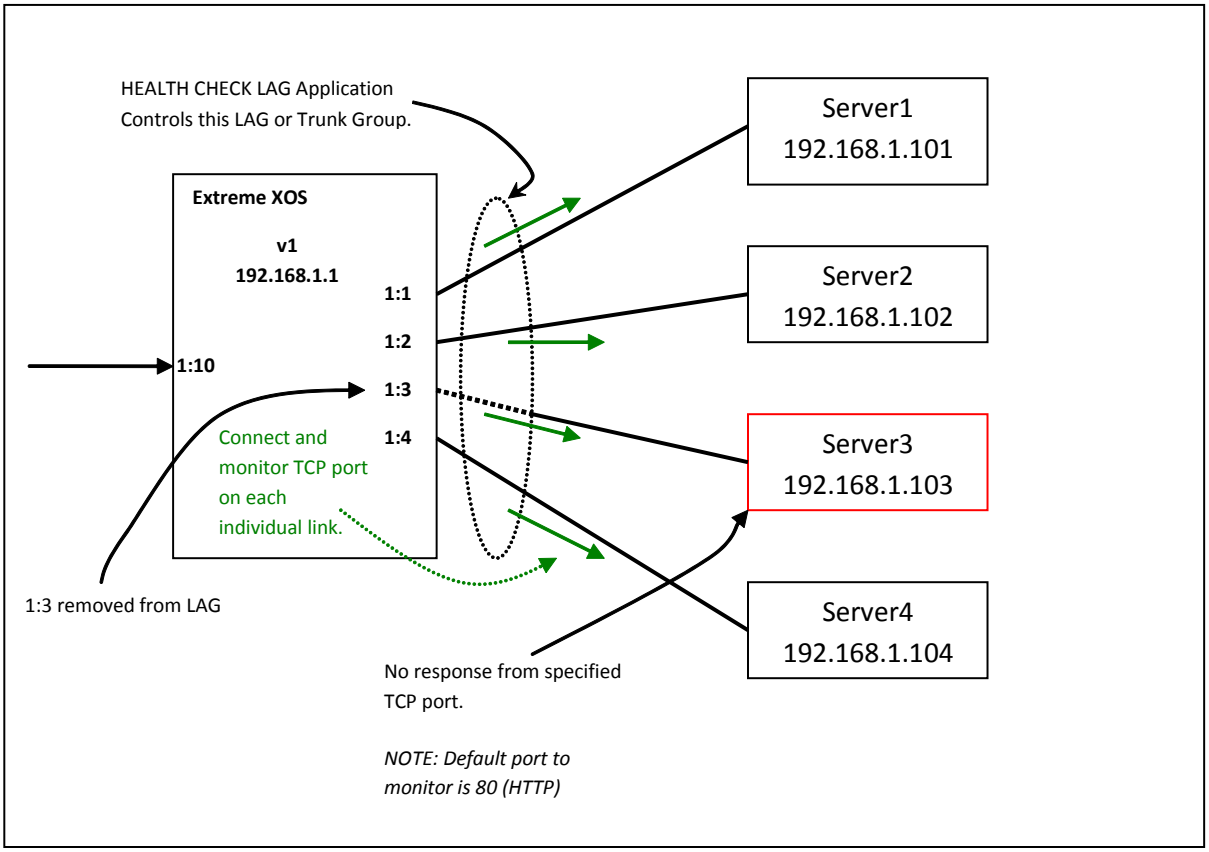
The Health Check LAG application allows you to create a link aggregation group where individual member links can monitor a particular TCP IP address and TCP port. When connectivity to the TCP IP address and TCP port fails, the member link is removed from the link aggregation group.

Establishing the status of a TCP connectivity is based on standard TCP socket connections. As long as the switch can establish a TCP connection to the target switch and TCP port, the connection is considered up. The TCP connection will retry based on the configured frequency and miss settings.

A typical use case for this application is when a user wishes to connect each member link to a Security Server to validate traffic. Each member link of the Health Check LAG is connected to an individual Security Server. The LAG is added to a VLAN on the same subnet as the Security Server IP addresses they wish to monitor. Each member port is configured to monitor a particular IP address and TCP port. The Health Check LAG application attempts to do a TCP connect to each IP/TCP port through each member port. The Health Check LAG, by virtue of the sharing algorithm, will load balance traffic across the member links. If a TCP connection cannot be established through the member link, the port is removed from the aggregator and traffic through that particular link is redistributed to the other LAG member links.

Figure 1 displays an example of a Health Check LAG.

Figure 1: Health Check LAG Example



Configuring Health Check Link Aggregation

To configure Health Check link aggregation you must first create a LAG. One port in the LAG serves as the logical port for the LAG and is the reference port used in configuration commands.

When you create the LAG, no monitoring is initially configured. The LAG is created in the same way that a static LAG is created and if no monitoring if ever created, this LAG behaves like a static LAG.

1 Create a LAG using the following command:

```
enable sharing <port> grouping <port_list> {algorithm [port-based | address-based
{L2 | L3 | L3_L4}]} {lacp | health-check}
```

The port you assign using the <port> parameter becomes the logical port for the link aggregation group and the LAG Group ID when using Health Check link aggregation. This logical port must also be included in the port list of the grouping itself.

2 Configure monitoring for each member port using the following command:

```
configure sharing health-check member-port <port> add tcp-tracking <IP Address>
{tcp-port <TCP Port> frequency <sec> misses <count>}
```

If the TCP-port, frequency, or misses are not specified, the defaults described in the *ExtremeXOS Command Reference Guide* are used.

3 Add the LAG to a VLAN whose subnet is the same as the configured tracking IP addresses.

```
configure vlan <vlan> add port <lag port> [tagged | untagged]
```

All of the tracking IP addresses must be in the same subnet in which the LAG belongs.

NOTE

VLANs to which Health Check LAG ports are to be added must be configured in loopback mode. This is to prevent the vlan interface from going down if all ports are removed from the Health Check LAG. In a normal LAG when all ports are removed from the aggregator, the trunk is considered DOWN. As a consequence, if this were the only port in the VLAN, the VLAN interface would be brought DOWN as well. In the Health Check LAG situation, this would cause the TCP monitoring to fail because the L3 vlan interface used by TCP monitoring would no longer send or receive TCP data.

The following commands are used to modify the configured Health Check LAG.

1 Delete the monitoring configuration for a member port using the following command:

```
configure sharing health-check member-port <port> delete tcp-tracking <IP Address>
{tcp-port <TCP Port>}
```

2 Enable or disable monitoring for a member port in the Health Check LAG using the following command:

```
configure sharing health-check member-port <port> [disable | enable] tcp-tracking
```

Health Check LAG Example

The following example creates a Health Check LAG of 4 ports:

```
create vlan v1
configure v1 ip 192.168.1.1/24
enable sharing 5 grouping 5-8 health-check
enable loopback-mode v1
configure v1 add port 5
configure sharing health-check member-port 5 add track-tcp 192.168.1.101 tcp-port 8080
configure sharing health-check member-port 6 add track-tcp 192.168.1.102 tcp-port 8080
configure sharing health-check member-port 7 add track-tcp 192.168.1.103 tcp-port 8080
configure sharing health-check member-port 8 add track-tcp 192.168.1.104 tcp-port 8080
```

Displaying Health Check Link Aggregation

To display information for a health check LAG, use the following command:

```
show sharing health-check
```

Health Check Link Aggregation Commands

Following are CLI commands for Health Check Link Aggregation.

configure sharing add ports

```
configure sharing <port> add ports <port_list>
```

Description

Adds ports to a load-sharing, or link aggregation, group. By using link aggregation, you use multiple ports as a single logical port. Link aggregation also provides redundancy because traffic is redistributed to the remaining ports in the link aggregation group (LAG) if one port in the group goes down.

Syntax Description

port	Specifies the logical port for a load-sharing group or link aggregation group (LAG). This number also functions as the LAG Group ID.
port_list	Specifies one or more ports or slots and ports to be grouped in the LAG.

Default

N/A.

Usage Guidelines

NOTE

You must create a LAG (or load-sharing group) before you can configure the LAG. To create a LAG, see `enable sharing <port> grouping <port_list> {algorithm [port-based | address-based {L2 | L3 | L3_L4}]} {lacp | health-check}`.

Use this command to dynamically add ports to a load-sharing group, or link aggregation group (LAG).

vMAN ports can belong to LAGs. If any port in the LAG is enabled for vMAN, all ports in the group are automatically enabled to handle jumbo size frames. Also, vMAN is automatically enabled on all ports of the untagged LAG.

To verify your configuration, use the `show ports sharing` command.

NOTE

All ports that are designated for the LAG must be removed from all VLANs prior to configuring the LAG.

Summit family of switches only (does not apply to SummitStack). The following guidelines apply to link aggregation on the Summit family of switches:

- One static LAG can contain up to 8 ports.
- An LACP LAG can include a maximum of 16 ports; out of these up to 8 can be selected links and the remaining 8 will be standby links.
- A Health Check LAG can contain up to 8 ports.

- The default load-sharing algorithm is L2 address-based aggregation. Any broadcast, multicast, or unknown unicast packets are transmitted differently depending on the device you are using.
  - On the Summit X450 series switches, these packets are transmitted on a single port of a LAG.
  - On the Summit X150, X250e, X350, X450a, X450e, and X650 series switches, these packets are distributed across all members of a LAG.
- The maximum number of LAGs is 32.
- The available address-based parameters on the Summit family of switches are as follows:
  - Summit X450 series switches—L2 for Layer 2 and L3 for Layer 3. If the packet is not IP, the switch applies the Layer 2 algorithm, which is the default setting.
  - Summit X150, X250e, X350, X450a, X450e, and X650 series switches—L2 for Layer 2, L3 for Layer 3, and L3_L4 for Layer 3/Layer 4.

NOTE

You cannot configure port-based load sharing algorithm on the Summit family of switches; you configure only address-based load-sharing algorithms.

BlackDiamond 8800 series switch and SummitStack only. The following guidelines apply to link aggregation on the BlackDiamond 8800 series switch:

- A static LAG can include a maximum of 8 ports.
- An LACP LAG can include a maximum of 16 ports; out of these up to 8 can be selected links and the remaining 8 will be standby links.
- A Health Check LAG can include a maximum of 8 ports.
- Any broadcast, multicast, or unknown unicast packet is transmitted on a single port in the LAG.

NOTE

You cannot configure port-based load sharing algorithm on the BlackDiamond 8800 series switch and the Summit family of switches; you configure only address-based load-sharing algorithms.

- The available address-based parameters on the BlackDiamond 8800 series switch are L2 for Layer 2 and L3 for Layer 3. If the packet is not IP, the switch applies the Layer 2 algorithm, which is the default setting.
- Beginning with ExtremeXOS version 11.5 for the BlackDiamond 8800 series switches and ExtremeXOS version 12.0 for SummitStack, the maximum number of LAGs is 128 unless a 10G4X module is in use in a BlackDiamond 8800 series switch or a Summit X450-24t or X450-24x switch is in the SummitStack, in which case the maximum number of LAGs is 32.

NOTE

You cannot configure more than 32 LAGs on a BlackDiamond 8800 chassis with a 10G4X module running or that has a slot configured for the 10G4X module. You cannot configure more than 32 LAGs on a SummitStack that has a Summit X450-24t or X450-24x or that has a slot configured for either model.

If you attempt to configure more than 32 LAGs on a BlackDiamond 8800 chassis that contains an 10G4X module or has a slot configured for the 10G4X module, the system displays the following error message:

```
Error: Slot <slot_number> can support a maximum of 32 trunks
```

If you want to configure more than 32 LAGs, it is not necessary to remove the 10G4X or Summit X450 series module; however, you must *both* unconfigure the slot holding the module *and* disable the slot holding that module or remove the module (the disable slot command is not available on SummitStack). Use the following commands to unconfigure the slot and disable that slot:

```
unconfigure slot and disable slot
```

If you attempt to insert a 10G4X module into a BlackDiamond 8800 chassis or a SummitStack with a Summit X450 series module configured for more than 32 LAGs, the module fails the Init state with log error messages at the warning level similar to the following:

```
04/07/1921 23:52:28.29 <Warn:DM.Warning> MSM-A: Slot-8 FAILED (1) Error Max Load
Share Groups Exceeded(-48) from HAL on CardExec INIT(5) for slot
```

```
04/07/1921 23:52:28.29 <Warn:DM.Warning> MSM-A: Error Max Load Share Groups
Exceeded(-48) from HAL on CardExec INIT(5) for slot 8
```

Once you configure more than 32 LAGs, the module will not initialize even if you reduce the number of LAGs to 32; you must reboot the system or SummitStack first. The system logs an error message at the error level similar to the following when you must reduce the system (even if you reduced the number of LAGs to 32):

```
04/07/1921 23:52:28.29 <Erro:HAL.Card.Error> MSM-A: Slot 8 is not supported when
more than 32 load share groups have previously been configured.  A system reboot
is required to clear this condition.
```

BlackDiamond 10808 switch, BlackDiamond 12800 and 20808 series switches only. The following guidelines apply to LAGs on the BlackDiamond 10808, 12800, and 20808 series switches:

- A static LAG can include a maximum 16 ports.
- An LACP LAG can include a maximum of 32 ports; out of these up to 16 can be selected links and the remaining 16 will be standby links.
- A Health Check LAG can include a maximum of 16 ports.
- The maximum number of LAGs is 128.
- If you do not explicitly select an algorithm, the port-based scheme is used. However, the address-based algorithm has a more even distribution and is the recommended choice.

NOTE

You must use the `configure sharing address-based` *command to configure address-based load sharing on the BlackDiamond 10808, BlackDiamond 12800, and BlackDiamond 20808 series switches.*

Example

The following example adds port 3:13 to the LAG with the logical port 3:9 on a modular switch:

```
configure sharing 3:9 add port 3:13
```

History

This command was first available in ExtremeXOS 10.1.

Platform Availability

This command is available on all platforms.

configure sharing health-check member-port add tcp-tracking

```
configure sharing health-check member-port <port> add tcp-tracking <IP
Address> {tcp-port <TCP Port> frequency <sec> misses <count>}
```

Description

Configures monitoring for each member port of a health check LAG.

Syntax Description

port	Specifies the member port.
IP Address	Specifies the IP address to monitor.
TCP Port	Specifies the TCP port to watch. The default is port 80.
sec	Specifies the frequency in seconds at which tracking takes place. The default is 10 seconds.
count	Specifies the number of misses before a connection loss is reported. The default is 3 misses.

Default

N/A.

Usage Guidelines

To configure a health check LAG, you first create a health check type of LAG using the `enable sharing grouping` command. Then use this command to configure the monitoring for each member port. You can configure each member port to track a particular IP address, but only one IP address per member port.

To display the monitoring configuration for a health check LAG, use the show `sharing health-check` command.

To display the link aggregation configured on a switch, use the `show ports sharing` command.

Example

The following commands configure four different member ports:

```
# configure sharing health-check member-port 10 add track-tcp 10.1.1.1 tcp-port 23
# configure sharing health-check member-port 11 add track-tcp 10.1.1.2 tcp-port 23
# configure sharing health-check member-port 12 add track-tcp 10.1.1.3
# configure sharing health-check member-port 13 add track-tcp 10.1.1.4
```

When the TCP port, seconds, or counts are not specified, they default to the values described in the Syntax Description.

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on all platforms.

configure sharing health-check member-port delete tcp-tracking

```
configure sharing health-check member-port <port> delete tcp-tracking <IP
Address> {tcp-port <TCP Port>}
```

Description

Unconfigures monitoring for each member port of a health check LAG.

Syntax Description

port	Specifies the member port.
IP Address	Specifies the IP address.
TCP Port	Specifies the TCP port.

Default

N/A.

Usage Guidelines

Use this command to remove the monitoring configuration on the ports of a health check link aggregation group. Each port must be unconfigured separately, specifying the IP address and TCP port.

Example

The following command removes the configuration setting on port 12 that monitors IP address 10.1.1.3:

```
# configure sharing health-check member-port 12 delete track-tcp 10.1.1.3
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on all platforms.

configure sharing health-check member-port tcp-tracking

```
configure sharing health-check member-port <port> [disable | enable] tcp-
tracking
```

Description

Enables or disables configured monitoring on a member port of a health check LAG.

Syntax Description

port	Specifies the member port.

Default

N/A.

Usage Guidelines

This disables/enables monitoring on a particular member port. When monitoring is disabled, the member port is added back to the LAG if it has not already been added. This allows a member port to be added back to LAG even though connectivity to the host is down.

Example

The following command disables port 12:

```
configure sharing health-check member-port 12 disable tcp-tracking
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on all platforms.

enable sharing grouping

```
enable sharing <port> grouping <port_list> {algorithm [port-based |
address-based {L2 | L3 | L3_L4}]} {lacp | health-check}
```

Description

Enables the switch to configure port link aggregation, or load sharing. By using link aggregation, you use multiple ports as a single logical port. Link aggregation also provides redundancy because traffic is redistributed to the remaining ports in the LAG if one port in the group goes down. LACP allows the system to dynamically configure the LAGs.

Syntax Description

port	Specifies the master logical port for a load-sharing group or link aggregation group (LAG).
port_list	Specifies one or more ports or slots and ports to be grouped to the logical port.
port-based	Specifies link aggregation by port-based algorithm. NOTE: This parameter is available only on the BlackDiamond 10808 and the BlackDiamond 12800 series switches.
address-based	Specifies link aggregation by address-based algorithm.
L2	Specifies address-based link aggregation by Layer 2. This is the default value. NOTE: This parameter is available only on the BlackDiamond 8800 series switch, SummitStack, and the Summit family of switches.
L3	Specifies address-based link aggregation by Layer 3. NOTE: This parameter is available only on the BlackDiamond 8800 series switch, SummitStack, and the Summit X450 series switch.
L3_L4	Specifies address-based link aggregation by Layer 3 IP plus Layer 4 port. NOTE: This parameter is available only on the BlackDiamond 8000 a-series, c-series, and e-series modules and the Summit X250e, X450a, X450e, and X650 series switches (whether or not included in a SummitStack.
lacp	Specifies dynamic link aggregation, or load sharing, using the LACP.
health-check	Specifies a health check type of link aggregation group.

Default

Disabled.

Usage Guidelines

Link aggregation, or load sharing, allows you to increase bandwidth and availability between switches by using a group of ports to carry traffic in parallel between switches. The aggregation algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see the link aggregation group (LAG) as a single logical port. Groups can span multiple modules.

NOTE

All ports that are designated for the LAG must be removed from all VLANs prior to configuring the LAG.

You can enable and configure dynamic link aggregation, using LACP or health-check link aggregation. Static link aggregation is the default link aggregation method.

NOTE

Always verify the LACP configuration by issuing the `show ports sharing` *command; look for the ports listed as being in the aggregator.*

If a port in a LAG fails, traffic is redistributed to the remaining ports in the LAG. If the failed port becomes active again, traffic is redistributed to include that port.

Link aggregation must be enabled on both ends of the link, or a network loop will result.

NOTE

See ExtremeXOS Concepts Guide *for information on the interaction of port-based ACLs and LAGs of ports.*

Modular switch LAGs are defined according to the following rules:

- Although you can *reference* only the logical port of a LAG to a Spanning Tree Domain (STPD), *all* the ports of a load-sharing group actually belong to the specified STPD.
- When using link aggregation, you should always reference the logical port of the LAG when configuring or viewing VLANs. VLANs configured to use other ports in the LAG will have those ports deleted from the VLAN when link aggregation becomes enabled.

Link aggregation, or load-sharing, algorithms allow you to select the distribution technique used by the LAG to determine the output port selection. Algorithm selection is not intended for use in predictive traffic engineering.

- Port-based—Uses the ingress port to determine which physical port in the LAG is used to forward traffic out of the switch.
- Address-based—Uses addressing information to determine which physical port in the LAG to use for forwarding traffic out of the switch. Refer to `configure sharing address-based` for more information on using addressing information.

Summit X250e, X450a, X450e, and X650 series switches and SummitStack only. The following guidelines apply to link aggregation on the Summit X250e, X450a, X450e, and X650 series switches:

- One static LAG can contain up to 8 ports.
- An LACP LAG can include a maximum of 16 ports; out of these up to 8 can be selected links and the remaining 8 will be standby links.
- A Health Check LAG can contain up to 8 ports.
- The maximum number of LAGs is 128.
- The default load-sharing algorithm is L2 address-based aggregation. Any broadcast, multicast, or unknown unicast packet is distributed across all members in the LAG.
- The available address-based parameters on the Summit X250e, X450a, X450e, and X650 series switches are L2 for Layer 2 and L3_L4 for Layer 3 plus Layer 4. If the packet is not IP, the switch applies the Layer 2 algorithm, which is the default setting.
- Beginning with ExtremeXOS version 12.0, the maximum number of LAGs in a SummitStack is 128 unless an original X450 series module is in use in the stack, in which case the maximum number of LAGs is 32.

NOTE

You cannot configure port-based load sharing algorithm on Summit X450 series switches; you configure only address-based load-sharing algorithms.

Summit X450 series switch only. The following guidelines apply to link aggregation on the Summit X450 series switch:

- One static LAG can contain up to 8 ports.
- An LACP LAG can include a maximum of 16 ports; out of these up to 8 can be selected links and the remaining 8 will be standby links.
- A Health Check LAG can contain up to 8 ports.
- The maximum number of LAGs is 32.
- The default load-sharing algorithm is L2 address-based aggregation. Any broadcast, multicast, or unknown unicast packet is transmitted on a single port in the LAG.
- The available address-based parameters on the Summit X450 series switch are L2 for Layer 2 and L3 for Layer 3. If the packet is not IP, the switch applies the Layer 2 algorithm, which is the default setting.

NOTE

You cannot configure port-based load sharing algorithm on the Summit X450 series switch; you configure only address-based load-sharing algorithms.

BlackDiamond 8800 series switch only. The following guidelines apply to link aggregation on the BlackDiamond 8800 series switch:

- A static LAG can include a maximum of 8 ports.
- An LACP LAG can include a maximum of 16 ports; out of these up to 8 can be selected links and the remaining 8 will be standby links.
- A Health Check LAG can include a maximum of 8 ports.

NOTE

You cannot configure port-based load sharing algorithm on the BlackDiamond 8800 series switch and the Summit X450 series switches; you configure only address-based load-sharing algorithms.

- The available address-based parameters on the BlackDiamond 8800 series switch are L2 for Layer 2 and L3 for Layer 3.

  If the packet is not IP, the switch applies the Layer 2 algorithm, which is the default setting. Beginning with ExtremeXOS software version 11.2, the switch can use IPv6 addresses.
- The maximum number of LAGs is 32.
- Broadcast, multicast, or unknown unicast packets are transmitted differently depending on the device you are using:
  - On the BlackDiamond 8800 original-series modules, these packets are transmitted on a single port of a LAG.
  - On the BlackDiamond 8000 a-series, c-series, and e-series modules, these packets are distributed across all members of a LAG. The distribution of these packets depends on the type of the traffic. Broadcast, L2 multicast and unknown unicast traffic distribution is based on the source and

destination MAC addresses. IP multicast traffic distribution is based on the source and destination IP addresses. This behavior is not configurable.

- Beginning with ExtremeXOS version 11.5, the maximum number of LAGs is 128 unless a 10G4X module is in use in the chassis, in which case the maximum number of LAGs is 32.

NOTE

You cannot configure more than 32 LAGs on a BlackDiamond 8800 chassis with a 10G4X module running or that has a slot configured for the 10G4X module.

The following switch configurations support 32 LAGs:

- A BlackDiamond 8800 switch that contains an 10G4X module or has a slot configured for the 10G4X module
- A SummitStack that contains an original Summit X450 switch or has a slot configured for the X450 switch

If you attempt to configure more than 32 LAGs on a switch or stack that does not support larger configurations, the system displays the following error message:

```
Error: Slot <slot_number> can support a maximum of 32 trunks
```

If you want to configure more than 32 LAGs on a BlackDiamond 8800 switch, it is not necessary to remove the 10G4X module; however, you must *both* unconfigure the slot holding the 10G4X module *and* disable the slot holding that module or remove the 10G4X module. Use the following commands to unconfigure the slot and disable that slot:

unconfigure slot and disable slot

If you want to configure more than 32 LAGs on a SummitStack, you must remove all original Summit X450 switches from the active topology.

If you attempt to insert a 10G4X module into a BlackDiamond 8800 chassis configured for more than 32 LAGs, or if you attempt to add an original X450 module into a SummitStack with more than 32 LAGs, the module fails the Init state with log error messages at the warning level similar to the following:

```
04/07/1921 23:52:28.29 <Warn:DM.Warning> MSM-A: Slot-8 FAILED (1) Error Max Load Share
Groups Exceeded(-48) from HAL on CardExec INIT(5) for slot
04/07/1921 23:52:28.29 <Warn:DM.Warning> MSM-A: Error Max Load Share Groups Exceeded(-
48) from HAL on CardExec INIT(5) for slot 8
```

Once you configure more than 32 LAGs on a BlackDiamond 8800 chassis or SummitStack, the 10G4X or original Summit X450 series module will not initialize even if you reduce the number of LAGs to 32; you must reboot the system or stack first. The system logs an error message at the error level similar to the following when you must reduce the system (even if you reduced the number of LAGs to 32):

```
04/07/1921 23:52:28.29 <Erro:HAL.Card.Error> MSM-A: Slot 8 is not supported when more
than 32 load share groups have previously been configured.  A system reboot is
required to clear this condition.
```

When you have BlackDiamond 8800 original-series modules and BlackDiamond 8000 a-series, c-series, and e-series modules in the same chassis, or when you have original Summit X450 switches and X650,

X450a, X450e, or X250e switches in the same SummitStack, the configured algorithm may behave differently, as shown in the following:

Configured algorithm:	BlackDiamond 8800 original-series module or Summit X450 series switch	BlackDiamond 8000 a-series, c-series, and e-series modules or SummitStack with Summit X650, X450a, X450e, or X250e switch
L2	L2	L2 (with flooding and multicast traffic balanced)
L3	L3	L3 and L4 ports
L3_L4	L3	L3 and L4 ports

BlackDiamond 10808, BlackDiamond 12800, and BlackDiamond 20808 series switches only. The following guidelines apply to load sharing on the BlackDiamond 10808, 12800 and 20808 series switches:

- A static LAG can include a maximum of 16 ports.
- An LACP LAG can include a maximum of 32 ports; out of these up to 16 can be selected links and the remaining 16 will be standby links.
- A Health Check LAG can include a maximum of 16 ports.
- The maximum number of LAGs is 128.

On the BlackDiamond 10808, 12800, and 20808 series switches, if you do not explicitly select an algorithm, the port-based scheme is used. However, the address-based algorithm has a more even distribution and is the recommended choice.

NOTE

You must use the `configure sharing address-based` *command to configure address-based load sharing on the BlackDiamond 10808 and 12800 series switches.*

Example

The following example defines a static link aggregation group (LAG) on a modular switch that contains ports 9 through 12 on slot 3, ports 7 through 10 on slot 5, and uses the first port on slot 3 as the logical port 9 on a modular switch:

```
enable sharing 3:9 grouping 3:9-3:12, 5:7-5:10
```

In this example, logical port 3:9 represents physical ports 3:9 through 3:12 and 5:7 through 5:10.

The following example defines a dynamic LAG on a stand-alone switch containing ports 10 through 15, with port 10 being the logical port:

```
enable sharing 10 grouping 10-15 lacp
```

The following example defines a health check LAG containing ports 10 through 13 with port 10 as the master logical port and specifies address-based link aggregation by Layer 3 IP plus Layer 4 port:

```
enable sharing 10 grouping 10,11,12,13 algorithm address L3_L4 health-check
```

To configure a health-check LAG, refer to the `configure sharing health-check member-port add tcp-tracking` command.

History

This command was first available in ExtremeXOS 10.1.

The address-based algorithm was added in ExtremeXOS 11.0.

The L2 and L3 optional parameters were added in ExtremeXOS 11.1.

IPv6-compatibility was added in ExtremeXOS 11.2.

Dynamic link aggregation, using LACP, was added in ExtremeXOS 11.3.

The L3_L4 optional parameter was added in ExtremeXOS 11.5.

SummitStack functionality was added in ExtremeXOS 12.0.

Health-check link aggregation was added in ExtremeXOS 12.1.3.

Platform Availability

This command is available on all platforms.

show ports sharing

```
show ports sharing
```

Description

Displays port load-sharing groups, or link aggregation groups (LAGs).

Syntax Description

This command has no arguments or variables.

Default

N/A.

Usage Guidelines

Output from this command displays the following information:

- Config Master—The port that is configured as the master logical port of the link aggregation group (LAG). This number is also the LAG group ID.
- Current Master—In LACP, this is the port that is currently the LAG group ID, or master logical port for the LAG.
- Agg Control—This is the aggregation control for the specified LAG; it can be either static, LACP or health-check. In LACP, it is the aggregation control for the specified LAG.
- Ld Share Algorithm—The algorithm used for the link aggregation. The available link aggregation algorithms vary among platforms; see the *ExtremeXOS Concepts Guide* for more information.
- Ld Share Group—The specific ports that belong to each LAG, or the port numbers in the trunk. A port can belong to only one LAG, either static or dynamic.
- Agg Mbr—In LACP, this shows whether the port has been added to the aggregator or not; it will be either Y for yes or - for no.
- Link State—This is the current status of the link
- Link Up transitions—Number of times the link has cycled through being up, then down, then up.

Example

The following command displays link aggregation on the switch:

```
show ports sharing
```

The following is sample output from this command on a Summit X450 series switch:

```
Load Sharing Monitor
Config    Current    Agg       Ld Share    Ld Share  Agg   Link    Link Up
Master    Master     Control   Algorithm   Group     Mbr   State   transitions
================================================================================
     1      1        hlth-chk  L2          1          Y      A        1
                              L2          1          -      A        1
                              L2          1          Y      A        1
     5      5        LACP      L2          5          Y      A        3
                              L2          6          Y      A        3
                              L2          7          Y      A        3
                              L2          8          Y      A        3
                              L2          9          -      A        3
                              L2          10         -      A        3
    12               Static    L2          12         -      R        0
                              L2          13         -      R        0
================================================================================
Link State: A-Active, D-Disabled, R-Ready, NP-Port not present, L-Loopback
Load Sharing Algorithm: (L2) Layer 2 address based, (L3) Layer 3 address based,
(L3_L4) Layer 3 address and Layer 4 port based
Default algorithm: L2
Number of load sharing trunks: 2
```

History

This command was first available in ExtremeXOS 10.1.

The LACP feature was added in ExtremeXOS 11.3.

The Health Check LAG was added in ExtremeXOS 12.1.3

Platform Availability

This command is available on all platforms.

New FEFI CLI Command

The following CLI command enables and disables far-end-fault-indication (FEFI).

configure ports far-end-fault-indication

```
configure ports <port_list> far-end-fault-indication [on | off]
```

Description

Enables/disables far-end-fault-indication.

Syntax Description

port_list	Specifies one or more ports or slots and ports.

Default

FEFI is disabled by default.

Usage Guidelines

Use this command to enable FEFI. When enabled, FEFI signals to the remote end on detecting single link (RX) failure/recovery.

The command is supported on:

- FX/LX and 100 FX GBICS. FX/LX GBIC should be operating in 100M mode.
- Summit X450-24x and Summit X450a-24x platforms.
- Non-combo GBIC ports, that is, ports 5-24 on the Summit X450-24x and ports 1-20 on the Summit X450a-24x. If an attempt is made to use this command on combo ports, it is rejected.

Since the GBICs can be plugged and removed, a warning message is displayed in the syslog when a media type changes from FX/LX and FX to another media type. The warning messaage indicates that FEFI mode is enabled but is not useful for the new media type.

The current status is displayed in the `show ports information detail` command.

Example

The following command enables FEFI on port 1:

```
configure ports 1 far-end-fault-indication on
```

History

This command was first available in ExtremeXOS 12.1.3.

Platform Availability

This command is available on the Summit X450-24x and X450a-24x platforms.

New Features or Feature Enhancements in ExtremeXOS 12.1.2.17

Following are the new features or feature enhancements supported in ExtremeXOS 12.1.2.17. These features are documented in detail in the ExtremeXOS 12.1.2 versions of the *ExtremeXOS Concepts Guide* and the *ExtremeXOS Command Reference Guide*, unless otherwise noted.

- Connectivity Fault Management (CFM) is now available on SummitStack and BlackDiamond 8800 series switches.
- EAPS updates to support multicast.

  The following commands have been added to provide control of rapid multicast convergence after EAPS topology changes:

  - `configure eaps multicast add-ring-ports [on | off]`
  - `configure eaps multicast send-igmp-query [on | off]`
  - `configure eaps multicast temporary-flooding [on | off]`
  - `configure eaps multicast temporary-flooding duration <seconds>`

  See the *ExtremeXOS Command Reference, Software Version 12.1.2* for further details.

  The `show eaps` command has been modified to display the configuration of these controls and the EAPS chapter in the Concepts guide has been restructured.
- IS-IS SNMP support.
- 802.1Q Limitation on BlackDiamond 10808 and 12800 Series Switches:

  Only 802.1Q tags of valid VLANs configured on a switch can exist as arguments to the `vlan-id` keyword in an ACL rule. If a VLAN is deleted from the switch, the corresponding VLAN ID needs to be removed from all policy files.
- Removed the following deprecated vMAN action modifiers from the *ExtremeXOS Concepts Guide, Software Version 12.1.2*, "vMANs and Tunneling."
  - `stag ethertype`
  - `lag-aggregation-hash`
- Added the following SNMP commands. See the *ExtremeXOS Command Reference, Software Version 12.1.2*, "Managing the Switch."
  - `enable snmp community`
  - `disable snmp community`

New Hardware Supported in ExtremeXOS 12.1.2.17

The following modules are supported in ExtremeXOS 12.1.2.17:

- XFP modules
  - ZR XFP
  - DWDM XFP

  Supported on the Summit XGM2-2xf option card in the Summit X450a, X450e, and X350 series switches; also on the 10G4Xa, 10G4Xc, and 10G8Xc modules in the BlackDiamond 8800 series switches.

New Features in ExtremeXOS 12.1

Following are the new features supported in ExtremeXOS 12.1. These features will be documented in detail in the ExtremeXOS 12.1 versions of the *ExtremeXOS Concepts Guide* or the *ExtremeXOS Command Reference Guide*, unless otherwise noted.

- The `show configuration` command now displays configuration changes made by a user to factory default settings
- ScreenPlay now supports a Dynamic ACL Editor and CLI shell

  To use the CLI Shell, you must first download and install the CLI Proxy application on your desktop. The CLI Proxy installer is available at the Tech Support web site.
- ACL byte counters as an alternative to ACL packet counters
- EAPS enhancements
  - ESD configurable timers
- Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)
- vMAN enhancements
  - Per VLAN IGMP snooping
  - Service Tag (STAG) EtherType
  - Tagged and untagged support
- vMAN ingress ACL support to enable and disable IGMP snooping
- VLAN enhancements:
  - Aggregation
  - Translation
  - Private VLANs
- Universal ports enhancements
  - EMS integration
  - Additional triggers
  - Actions
- Multicast VLAN Registration (MVR) scaling enhancements for IGMP
- Routing table enhancements
  - Implementation of multicast routing table
  - Segregation of unicast and multicast routing table
- PIM snooping
- MPLS enhancements
  - Hierarchical Virtual Private LAN Services (HVPLS) L2 VPNs
  - Static LSPs
  - Pseudo wire Virtual Circuit Connectivity Verification (VCCV)
  - Protected VPLS
- IS-IS v4 and IS-IS v6
- IPv6 ECMP load balancing—BlackDiamond 10808 and BlackDiamond 12800 series switches
- Extended IPv4 host cache by way of configurable LPM table size for:

  - BlackDiamond 8800 a-series, c-series, and e-series modules
  - Summit X250e
  - Summit X450a and X450e series
- IGMP filters
  - Limit number of active streams
- IGMPv1/v2 SSM mapping for PIM-SSM
- RSTP/MSTP
  - Performance improvement
  - Cisco interoperability
- DHCP Option 82 at Layer 2
- Network login enhancements
  - Configurable netlogin dot1x client reauthentication
  - Authentication failure VLAN
  - Authentication server unavailable VLAN
- Web-based network login enhancements
  - Logout fault-tolerance in case of lost keep-alive packets in the presence of a logout pop-up window
  - User configurable content-refresh keep-alive timer value
  - Proxy port support
    - URL redirection support for adding user-configurable TCP port numbers (such as 8080).
    - Configurable TCP port for redirect-page after a successful login.
  - Network login redirect page disabled
  - Custom image in logout popup window
  - Reauthentication on refresh, that is, credentials are reverified after a session refresh
  - Support for authentication failure VLAN and service unavailable VLAN
- CLI to blackhole FDB
  - Unicast
  - Multicast
- Static unicast FDB with multiple ports (using ACL and combining MAC entries when possible)
- Unicast Reverse Path Forwarding—for BlackDiamond 10808 and BlackDiamond 12800 series switches
- Mirroring enhancements
  - Remote mirroring
- BGP
  - Route refresh
  - Cease subcodes
  - Allow looped BGP AS-Path
  - Extended community
- Disable learning option for flooding (instead of dropping)
- Multicast MIBs, RFC 2933-2934
- Ping, traceroute MIB

- CLI scripting
- Policy-based routing (PBR) with multiple hops (with health checking)
- Fast Reroute Recovery (FRR)

  FRR for RSVP-TE is introduced in Extreme XOS 12.1.1 as an LSP protection capability as defined in RFC 4090. Testing continues for this feature to stabilize and optimize this capability for deployment in production networks. At this time, FRR should not be enabled in a production network. To protect against accidentally enabling this feature in a production network, the CLI command `enable mpls rsvp-te fast-reroute` is hidden. If you want to test FRR in a lab environment and provide feedback, contact Extreme Networks Technical Support. The FRR feature will be supported for production networks in a future release of ExtremeXOS software once testing is complete.
- Provider Backbone Bridging–Traffic Engineering (PBB-TE), 802.1ag
- IP security enhancements
  - Added source IP lockdown counter
  - DHCP bindings preservation across reboots

New Hardware Supported in ExtremeXOS 12.1.1.4

The following modules are supported in ExtremeXOS 12.1.1.4:

- BlackDiamond 8800 c-series modules
  - MSM-48c
  - 10G1Xc
  - G8Xc
  - G48Tc with optional S-POE for inline power
  - G48Xc
  - G24Xc
  - 10G8Xc
  - 10G4Xc
- G48Te2 with optional S-POE for inline power
- Summit X350

Supported Hardware

Refer to the Extreme Networks hardware installation guides for more information about supported hardware. The following tables list the software filenames for the hardware that requires software.

BlackDiamond 10808 Switch Component Support

BlackDiamond 10808 components supported with ExtremeXOS 12.1, and the minimum ExtremeXOS version required by the chassis to support each component, include:

Table 1: BlackDiamond 10808 Component Support

BlackDiamond Component	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-1	bd10k-12.1.4.2-patch1-8.xos	10.1.0	1.0.1.5
MSM-1XL	bd10k-12.1.4.2-patch1-8.xos	10.1.0	1.0.1.5
10G38	N/A	11.1.1	1.3.0.0
10G2H	N/A	11.2.0	1.3.0.0
10G6X	N/A	10.1.0	1.3.0.0
G20X	N/A	11.1.1	1.3.0.0
G60X	N/A	10.1.0	1.3.0.0
G60T	N/A	10.1.0	1.3.0.0
PSU Controller	N/A	10.1.0	N/A
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	10.1.0	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.3.2.6	N/A

Following are the part numbers for the BlackDiamond 10808 modules with the Rev. D ASIC:

Table 2: BlackDiamond 10808 I/O Modules with Part Numbers

I/O Module	8000 Level Part No.	9000 Level Part No.	Description	ExtremeXOS Required
G60T	804403-00, after Rev. 16	904015-00	BlackDiamond 10808 60-port 10/100/1000BASE-T RJ-45 Module	11.2.1.3
	804408-00, after Rev. 03	904015-10	BlackDiamond 10808 60-port 10/100/1000BASE-T RJ-45 Module	11.2.1.3
G60X	804402-00, after Rev. 16	904009-00/11	BlackDiamond 10808 60-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
	804404-00, after Rev. 03	904009-10	BlackDiamond 10808 60-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
G20X	804407-00, after Rev. 03	904020-10	BlackDiamond 10808 20-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
	804470-00, after Rev. 08	904020-00/11	BlackDiamond 10808 20-port 1000BASE-X SFP (mini-GBIC) Module	11.2.1.3
10G38	804410-00, after Rev. 03	904032-10	BlackDiamond 10808 2-port 10GBASE-X XENPAK Module	11.2.1.3
	804471-00, after Rev. 11	904032-00/11	BlackDiamond 10808 2-port 10GBASE-X XENPAK Module	11.2.1.3
10G2H	804406-00, after Rev. 09	904027-00/11	BlackDiamond 10808 Hybrid Module (2-port 10GBASE-X XENPAK, 20-port 1000BASE-X SFP, 20-port 10/100/1000BASE-T RJ-45)	11.2.1.3
	804411-00, after Rev. 03	904027-10	BlackDiamond 10808 Hybrid Module (2-port 10GBASE-X XENPAK, 20-port 1000BASE-X SFP, 20-port 10/100/1000BASE-T RJ-45)	11.2.1.3
10G6X	804405-00, after Rev. 18	904016-00/11	BlackDiamond 10808 6-port 10GBASE-X XENPAK Module	11.2.1.3
	804409-00, after Rev. 03	904016-10	BlackDiamond 10808 6-port 10GBASE-X XENPAK Module	11.2.1.3

BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8800 and BlackDiamond 8806 components supported with ExtremeXOS 12.1, and the minimum BootROM version required by the chassis to support each component, include:

Table 3: BlackDiamond 8800 Series of Switches Component Support

BlackDiamond 8810 and BlackDiamond 8806 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-G8X	bd8800-12.1.4.2-patch1-8.xos	11.1.1.9	1.0.1.7
G48Te	N/A	11.5.1.4	1.0.1.10
G48Pe	N/A	11.5.1.4	1.0.1.10
G48Ta	N/A	11.5.1.4	1.0.1.10
G48Xa	N/A	11.5.1.4	1.0.1.10
G48P	N/A	11.1.1.9	1.0.1.7
G48T	N/A	11.1.1.9	1.0.1.7
G48Tc	N/A	12.1.1.4	1.0.3.7
G48Te2	N/A	12.1.1.4	1.0.3.7
G48Xc	N/A	12.1.1.4	1.0.3.7
G24X	N/A	11.1.1.9	1.0.1.7
G24Xc	N/A	12.1.1.4	1.0.3.7
G8Xc	N/A	12.1.1.4	1.0.3.7
10G4X	N/A	11.1.1.9	1.0.1.7
10G4Xa	N/A	11.6.1.9	1.0.1.11
10G4Ca	N/A	12.0.1.11	1.0.1.11
10G4Xc	N/A	12.1.1.4	1.0.3.7
10G8Xc	N/A	12.1.1.4	1.0.3.7
10G1Xc	N/A	12.1.1.4	1.0.3.7
PSU Controller	N/A	11.1.1.9	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.1.1.9	N/A
600/900 W AC PSU (Model # 41050/PS 2431) (BlackDiamond 8806 only)	N/A	11.6.1.9	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.3.2.6	N/A
MSM-48	bd8800-12.1.4.2-patch1-8.xos	11.6.1.9	1.0.1.11
MSM-48c	bd8800-12.1.4.2-patch1-8.xos	12.1.1.4	1.0.3.7

NOTE

Upgrading the BootROM on a BlackDiamond 8810 or BlackDiamond 8806 switch is not automatic when you upgrade the software. You must be running the minimum required BootROM version or later. Use the install firmware command after upgrading the ExtremeXOS image to insure the BootROM is at the latest level.

BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802, BlackDiamond 12804, BlackDiamond 12802 R-Series, and BlackDiamond 12804 R-Series components supported with ExtremeXOS 12.1, and the minimum BootROM version required by the chassis to support each component, include:

Table 4: BlackDiamond 12800 Series Switches Component Support

BlackDiamond 12802/12804 Components	ExtremeXOS Filenames	ExtremeXOS Required	BootROM Version
MSM-5R (BlackDiamond 12804)	bd12k-12.1.4.2-patch1-8.xos	11.4.1.4	1.0.0.2
MSM-5R (BlackDiamond 12802)	bd12K-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.0.2
GM-20XTR	N/A	11.4.1.4	N/A
XM-38R	N/A	11.4.1.4	N/A
XM-2HR	N/A	12.1.1.4	N/A
MSM-5 (BlackDiamond 12804)	bd12k-12.1.4.2-patch1-8.xos	11.4.1.4	1.0.0.2
MSM-5 (BlackDiamond 12802)	bd12k-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.0.2
MSM-6R	bd12k-12.1.4.2-patch1-8.xos	12.0.2.25	1.0.1.8
GM-20XT	N/A	11.4.1.4	N/A
GM-20T	N/A	11.4.1.4	N/A
PSU Controller	N/A	11.4.1.4	2.13
700/1200 W AC PSU (Model # 60020/PS 2336)	N/A	11.4.1.4	N/A
1200 W DC PSU (Model # 60021/PS 2350)	N/A	11.4.1.4	N/A

Summit X150 and X350 Component Support

Summit X150 and X350 series components supported with ExtremeXOS 12.1, and the minimum BootROM version required by the chassis to support each component, include:

Table 5: Summit X150 and X350 Component Support

Summit X150 and X350 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X150-24t	summitX-12.1.4.2-patch1-8.xos	12.0.2.25	1.0.3.1
Summit X150-48t	summitX-12.1.4.2-patch1-8.xos	12.0.2.25	1.0.3.1
Summit X150-24p	summitX-12.1.4.2-patch1-8.xos	12.0.2.25	1.0.3.1
Summit X350-24t	summitX-12.1.4.2-patch1-8.xos	12.0.3.16	1.0.3.1
Summit X350-48t	summitX-12.1.4.2-patch1-8.xos	12.0.3.16	1.0.3.1

Summit X250e Component Support

Summit X250e components supported with ExtremeXOS 12.1, and the minimum BootROM version required by the chassis to support each component, include:

Table 6: Summit X250e Component Support

Summit X250 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X250e-24p	summitX-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.3.0
Summit X250e-48p	summitX-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.3.0
Summit X250e-24t	summitX-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.3.0
Summit X250e-48t	summitX-12.1.4.2-patch1-8.xos	12.0.1.11	1.0.3.0
Summit X250e-24x	summitX-12.1.4.2-patch1-8.xos	12.0.2.25	1.0.3.1
Summit X250e-24tDC	summitX-12.1.4.2-patch1-8.xos	12.0.3.16	1.0.3.1
Summit X250e-24xDC	summitX-12.1.4.2-patch1-8.xos	12.0.3.16	1.0.3.1
Summit X250e-48tDC	summitX-12.1.4.2-patch1-8.xos	12.0.3.16	1.0.3.1

Summit X450 Component Support

Summit X450 components supported with ExtremeXOS 12.1, and the minimum BootROM version required by the chassis to support each component, include:

Table 7: Summit X450 Component Support

Summit X450 Components	ExtremeXOS Filenames	Minimum ExtremeXOS Required	Minimum BootROM Version
Summit X450a Series			
Summit X450a-48t	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	1.0.2.2
Summit X450a-48tDC	summitX-12.1.4.2-patch1-8.xos	11.6.1.9	1.0.2.2
Summit X450a-24t	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	1.0.2.2
Summit X450a-24tDC	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	1.0.2.2
Summit X450a-24xDC	summitX-12.1.4.2-patch1-8.xos	11.6.1.9	1.0.2.2
Summit X450a-24x	summitX-12.1.4.2-patch1-8.xos	11.6.1.9	1.0.2.2
Summit X450e Series			
Summit X450e-24p	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	1.0.2.2
Summit X450e-48p	summitX-12.1.4.2-patch1-8.xos	11.6.1.9	1.0.2.2
Summit X450 Series			
Summit X450-24x	summitX-12.1.4.2-patch1-8.xos	11.2.2.4	1.0.0.9
Summit X450-24t	summitX-12.1.4.2-patch1-8.xos	11.2.2.4	1.0.0.9
Option Cards			
XGM-2xn	summitX-12.1.4.2-patch1-8.xos	N/A	N/A
XGM2-2xn	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	
XGM2-2xf	summitX-12.1.4.2-patch1-8.xos	11.5.1.4	

NOTE

Upgrading the BootROM on a Summit X450 switch is not automatic when you upgrade the software.You must be running the minimum required BootROM version. Use the `download bootrom` *command to download a BootROM image.*

SFP (Mini-GBIC) Support

SFPs supported on the BlackDiamond 8810 and BlackDiamond 8806 switches with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 8: BlackDiamond 8800 Series of Switches SFP Support

SFP	ExtremeXOS Required
1000BASE-T SFP	11.1.1.9
SX SFP	11.1.1.9
LX SFP	11.1.1.9
ZX SFP	11.1.1.9
100FX/1000LX SFP	11.3.1.3
100FX SFP	11.4.3.4 or 11.5.2.10 (not supported in 11.5.1.4)
1000BX SFP	11.4.1.4
LX100 SFP	12.0.1.11
10/100/1000BASE-T Copper SFP	12.0.2.25

SFPs supported on the BlackDiamond 10808 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include

Table 9: BlackDiamond 10808 Switch SFP Support

SFP	ExtremeXOS Required
LX100 SFP	12.0.1.11
SX SFP	10.1.0
LX SFP	10.1.0
ZX SFP	10.1.0
1000BASE-T SFP	11.1.1.9
1000BX SFP	11.6.1.9

SFPs supported on the BlackDiamond 12804 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 10: BlackDiamond 12804 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	11.4.1.4
LX SFP	11.4.1.4
ZX SFP	11.4.1.4
1000BASE-T SFP	11.4.1.4

Table 10: BlackDiamond 12804 Switch SFP Support

SFP	ExtremeXOS Required
1000BX SFP	11.6.1.9
LX100 SFP	12.0.1.11
100FX/1000LX SFP	11.6.1.9

SFPs supported on the BlackDiamond 12802 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 11: BlackDiamond 12802 Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	12.0.1.11
LX SFP	12.0.1.11
ZX SFP	12.0.1.11
1000BASE-T SFP	12.0.1.11
1000BX SFP	12.0.1.11
LX100 SFP	12.0.1.11
100FX/1000LX SFP	12.0.1.11

SFPs supported on the Summit X150 series switches with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 12: Summit X150 Series Switches SFP Support

SFP	ExtremeXOS Required
100BASE-FX	12.0.2.25
100BASE-BX SFP	12.0.2.25
100BASE LX10 SFP	12.0.2.25
SX SFP	12.0.2.25
LX SFP	12.0.2.25
ZX SFP	12.0.2.25
LX100 SFP	12.0.2.25
1000BX SFP	12.0.2.25

SFPs supported on the Summit X350 series switches with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 13: Summit X350 Series Switches SFP Support

SFP	ExtremeXOS Required
SX SFP	12.0.3.16
LX SFP	12.0.3.16
ZX SFP	12.0.3.16
LX100 SFP	12.0.3.16
1000BX SFP	12.0.3.16

SFPs supported on the Summit X450 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 14: Summit X450 Switch SFP Support

SFP	ExtremeXOS Required
10/100/1000BASE-T Copper SFP **Note**: Not supported on combo ports.	12.0.2.25
SX SFP	11.2.2.4
LX SFP	11.2.2.4
ZX SFP	11.2.2.4
1000BASE-T SFP	11.2.2.4
100FX SFP **Note**: Not supported on combo ports.	11.4.3.4 or 11.5.2.10 (not supported in 11.5.1.4)
100FX/1000LX SFP **Note**: Not supported on combo ports.	11.3.1.3
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X450a switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 15: Summit X450a Switch SFP Support

SFP	ExtremeXOS Required
10/100/1000BASE-T Copper SFP **Note**: Not supported on combo ports.	12.0.2.25
SX SFP	11.2.2.4
LX SFP	11.2.2.4
ZX SFP	11.2.2.4
100FX SFP **Note**: Not supported on combo ports.	11.6.1.9
100FX/1000LX SFP • Summit X450a-24x, ports 1 through 20 **Note**: Not supported on combo ports.	11.6.1.9
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X450e switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 16: Summit X450e Switch SFP Support

SFP	ExtremeXOS Required
SX SFP	11.6.1.9
LX SFP	11.6.1.9
ZX SFP	11.6.1.9

Table 16: Summit X450e Switch SFP Support

SFP	ExtremeXOS Required
LX100 SFP	12.0.1.11
1000BX SFP	11.6.1.9

SFPs supported on the Summit X250e switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 17: Summit X250e SFP Support

SFP	ExtremeXOS Required
SX SFP, ports 25 and 26	12.0.2.25
LX SFP, ports 25 and 26	12.0.2.25
ZX SFP, ports 25 and 26	12.0.2.25
LX100 SFP, ports 25 and 26	12.0.2.25
1000BX SFP, ports 25 and 26	12.0.2.25
100BASE FX (FE ports) SFP, ports 1 through 26 **Note**: Not supported on combo ports.	12.0.2.25
100BASE BX SFP, ports 1 through 26 **Note**: Not supported on combo ports.	12.0.2.25
100BASE LX10 SFP, ports 1 through 26 **Note**: Not supported on combo ports.	12.0.2.25

XENPAK Module Support

XENPAK modules supported on the BlackDiamond 8800 series of switches with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 18: BlackDiamond 8800 Series of Switches XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.1.1.9
ER	11.1.1.9
SR	11.1.1.9
LX4	11.3.1.3
ZR	11.3.1.3
CX4	12.0.1.11

XENPAK modules supported on the BlackDiamond 10808 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 19: BlackDiamond 10808 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.1.1.9
ER	11.1.1.9

Table 19: BlackDiamond 10808 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.1.1.9
LX4	11.3.1.3
ZR	11.3.1.3
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12804 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 20: BlackDiamond 12804 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	11.4.1.4
ER	11.4.1.4
SR	11.4.1.4
LX4	11.4.1.4
ZR	11.4.1.4
LW	11.4.1.4

XENPAK modules supported on the BlackDiamond 12802 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include

Table 21: BlackDiamond 12802 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
LR	12.0.1.11
ER	12.0.1.11
SR	12.0.1.11
LX4	12.0.1.11
ZR	12.0.1.11
LW	12.0.1.11

XENPAK modules supported on the Summit X450 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 22: Summit X450 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.3.1.3
LR	11.3.1.3
ER	11.3.1.3
LX4	11.3.1.3
ZR	11.3.1.3

XENPAK modules supported on the Summit X450a switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 23: Summit X450a Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	11.6.1.9
LX4	11.6.1.9
ZR	11.6.1.9
LW	11.6.1.9
CX4	12.0.1.11

XENPAK modules supported on the Summit X450e switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 24: Summit X450e Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	11.5.1.4
LX4	11.5.1.4
ZR	11.5.1.4
CX4	12.0.1.11

XENPAK modules supported on the Summit X350 switch with ExtremeXOS 12.1, and the minimum ExtremeXOS version required, include:

Table 25: Summit X350 Switch XENPAK Support

XENPAK Module	ExtremeXOS Required
SR	12.0.3.16
LR	12.0.3.16
ER	12.0.3.16
LX4	12.0.3.16
ZR	12.0.3.16

XENPAKs not supplied by Extreme Networks will show up as “Unsupported Optic Module” in the `show port x:y` information detail and `show port x:y configuration` command output.

XFP Module Support

XFP modules supported on the BlackDiamond 8800 series of switches with ExtremeXOS 12.1, the minimum ExtremeXOS version required include:

Table 26: BlackDiamond 8800 Series of Switches XFP Support

XFP Module	ExtremeXOS Required
SR	11.6.1.9
LR	11.6.1.9
ER	12.0.2.25
DWDM	12.1.2.17
ZR	12.1.2.17

XFP modules supported on the Summit X450a and X450e series switch with ExtremeXOS 12.1, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 27: Summit X450a and X450e Series Switch XFP Support

XFP Module	ExtremeXOS Required
SR	11.5.1.4
LR	11.5.1.4
ER	12.0.2.25
DWDM	12.1.2.17
ZR	12.1.2.17

XFP modules supported on the Summit X350 switch with ExtremeXOS 12.1, the minimum ExtremeXOS version required, and the manufacturers supported include:

Table 28: Summit X350 Switch XFP Support

XFP Module	ExtremeXOS Required
SR	12.0.3.16
LR	12.0.3.16
ER	12.0.3.16
DWDM	12.1.2.17
ZR	12.1.2.17

Summit X150 and X350 Series Switch Software Details

The Summit X150 and X350 series switches have a reduced feature set as compared to the Summit X250 series switches. Summit X150 series switches are supported from ExtremeXOS 12.0.2.25 release onwards and Summit X350 series switches are supported from ExtremeXOS 12.0.3 onwards. They support L2 Edge license and cannot be upgraded to higher license levels. For more details on licensing, see Appendix A, "ExtremeXOS Software Licenses," in the *ExtremeXOS Concepts Guide.*

ExtremeXOS Command Line Support

The following is true for all Summit X150 and X350 series switches:

- Summit X150 and X350 series switches do not support L3 functionality; this platform does not support CLI commands for L3 functionality.
- Summit X150 and X350 series switches do not support stacking; all CLI commands for stacking are not supported on this platform.
- Summit X150 and X350 series switches do not support IP forwarding; however, CLI commands that configure IP addresses function in order to access the management functionality of the switch are supported.
- Upgrade or trial licensing is not available on the Summit X150 and X350 series switches.

Supported Commands on the Summit X150 and X350 Series Switches

Table 29 contains the list of CLI commands supported on the Summit X150 and X350 series switches.

Table 29: Summit X150 and X350 Supported Commands

Command	Description
check	Check policy syntax
policy	Policy
clear	Clear system configuration
access-list	Access list
account	Login account
counters	Statistics
cpu-monitoring	CPU utilization
debug	Debug command
eaps	EAPS (Ethernet Automatic Protection Switching)
elrp	ELRP (Extreme Loop Recovery Protocol)
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESRP (Extreme Standby Router Protocol)
fdb	FDB
igmp	IGMP protocol
inline-power	Inline-power
ip-security	IP security
iparp	IP ARP command
ipmc	IP multicast help
l2stats	Layer 2 stats
lacp	LACP (Link Aggregation Control Protocol)
license-info	License information in EEPROM
log	Clear log message for memory-target
mld	MLDP (Multicast Listener Discovery Protocol)
neighbor-discovery	IPv6 neighbor
netlogin	Show network login specific information

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
session	Session
sys-recovery-level	Clear persistent sys-recovery-level
vlan	VLAN
<esrpDomain>	ESRP domain name
<vlan_name>	VLAN name
configure	Configure running system information
access-list	Access list
account	Login account
banner	System login banner
bootprelay	Configure BOOTP relay service
cli	CLI
cpu-transmit-priority	CPU transmit priority
debug	Debug information, core files
diffserv	Diffserv
dns-client	DNS Client
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching)
edp	EDP
egress	Egress
elrp-client	ELRP (Extreme Loop Recovery Protocol) client
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESRP (Extreme Standby Router Protocol)
failsafe-account	Configure the failsafe account
fdb	FDB
forwarding	Configure settings for hardware forwarding
idletimeout	Timeout for idling configuration session
igmp	IGMP
inline-power	Inline-power
ip-mtu	IP MTU (Maximum Transmission Unit)
ip-security	IP security
iparp	IP ARP command
jumbo-frame-size	Jumbo-frame-size
lacp	LACP (Link Aggregation Control Protocol)
lldp	Configure LLDP specific settings
log	Configure log service
mac-lockdown-timeout	MAC lockdown timeout
meter	Ingress traffic metering
mirroring	Mirroring
mld	MLDP (Multicast Listener Discovery Protocol)
mstp	MSTP configuration

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
mvr	Multicast VLAN registration
neighbor-discovery	IPv6 neighbor
netlogin	Configure network login specific settings
ports	Ports
protocol	Protocol filter
qosprofile	QoS profile
qosscheduler	Set the QOS scheduling algorithm
radius	Configure RADIUS server
radius-accounting	Configure RADIUS accounting server
safe-default-script	Safe default script configuration
sflow	Disable sFLOW module
sharing	Sharing
snmp	SNMP help
snmpv3	Configure SNMPv3
sntp-client	Configure SNTP Client
ssl	SSL
stpd	STP domain
sys-health-check	System health check
sys-recovery-level	Recovery level on exception
syslog	Remote syslog target
tacacs	Configure TACACS+ Server
tacacs-accounting	Configure TACACS+ Accounting Server
telnet	Telnet daemon
time	System time
timezone	Time zone
trusted-ports	Trusted ports
trusted-servers	Trusted servers
tunnel	Tunnel
vlan	VLAN
vman	vMAN configuration
<eapsDomain>	EAPS domain name
<esrpDomain>	ESRP domain name
<metername>	Meter name
<qosprofile>	QoS profile
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan_name>	VLAN name
cp	Copy file
internal-memory	Location is internal storage
<old-name>	Old file name
create	Create system configuration

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
access-list	Dynamic rule
account	Login account
eaps	EAPS (Ethernet Automatic Protection Switching) domain
fdbentry	FDB entry
log	Configure log service
meter	ingress traffic metering
netlogin	Network login
protocol	Protocol
qosprofile	QoS Profile
stpd	STP domain
tunnel	Tunnel
vlan	VLAN configuration
vman	vMAN configuration
delete	Delete system configuration
access-list	Access-list
account	Login account
eaps	EAPS (Ethernet Automatic Protection Switching) domain
esrp	ESRP (Extreme Standby Router Protocol) domain
fdbentry	FDB entry
log	Configure log service
meter	Ingress traffic metering
netlogin	Netlogin
protocol	Protocol
qosprofile	QoS profile
stpd	STP domain
tunnel	Tunnel
vlan	VLAN configuration
vman	vMAN configuration
<eapsDomain>	EAPS domain name
<metername>	Meter name
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan-name>	VLAN name
disable	Disable running system setting
access-list	Access list
bootp	Configure BOOTP client
bootprelay	Enable BOOTP relay service
cli	CLI settings
cli-config-logging	CLI command logging
clipaging	Display command output one screen at a time
cpu-monitoring	Monitor system/process CPU utilization

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
dhcp	Configure DHCP client
diffserv	Diffserv
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching) domain
edp	EDP
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
elsm	ELSM (Extreme Link Status Monitoring)
flooding	Flooding
icmp	ICMP option
idletimeout	Timeout for idling configuration session
igmp	IGMP Protocol
inline-power	Inline-Power
ip-option	IP option
ip-security	IP Security
iparp	IP ARP command
iproute	IPROUTE HELP
jumbo-frame	Jumbo-frame
learning	Learning
lldp	Configure LLDP specific settings
log	Configure log service
loopback-mode	Loopback
mac-lockdown-timeout	MAC lockdown timeout
mirroring	Mirroring
mld	Multicast Listener Discovery Protocol
mvr	Multicast VLAN Registration
netlogin	Configure Network Login specific settings
ports	Port
radius	RADIUS client
radius-accounting	RADIUS client accounting
rmon	RMON CLI command
sflow	Disable sFlow module
sharing	Sharing
smartredundancy	Smart redundancy on a port (software redundant feature)
snmp	Configure SNMP specific settings
sntp-client	Enable SNTP client
stpd	STP domain
syslog	Configure syslog service
tacacs	TACACS+ Client
tacacs-accounting	TACACS+ Client Accounting
tacacs-authorization	TACACS+ Client CLI Authorization

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
telnet	Disable incoming telnet connections
udp-echo-server	Enable a UDP echo server
vlan	VLAN configuration
watchdog	Watchdog monitoring feature
web	WEB help
xml-cli	CLI-based XML configuration mode
xml-mode	Raw XML configuration mode
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<vlan-name>	VLAN name
download	Download system image
bootrom	BootROM
image	Image
ssl	SSL
edit	Edit file
policy	Policy
script	ExtremeXOS CLI script
enable	Enable running system setting
access-list	Access list
bootp	Configure BOOTP client
bootprelay	Enable BOOTP relay service
cli	CLI settings
cli-config-logging	CLI command logging
clipaging	Display command output one screen at a time
cpu-monitoring	Monitor system/process CPU utilization
dhcp	Configure DHCP client
diffserv	Diffserv
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
eaps	EAPS (Ethernet Automatic Protection Switching) domain
edp	EDP
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
elsm	ELSM (Extreme Link Status Monitoring)
esrp designated-carrier	ESRP designated carrier feature
flooding	Flooding
icmp	ICMP option
idletimeout	Timeout for idling configuration session
igmp	IGMP protocol
inline-power	Inline-power
ip-option	IP option
ip-security	IP security

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
iparp	IP ARP command
iproute	IPROUTE help
jumbo-frame	Jumbo-frame
learning	Learning
license	ExtremeXOS license or feature pack
lldp	Configure LLDP specific settings
log	Configure log service
loopback-mode	Loopback
mac-lockdown-timeout	MAC lockdown timeout
mirroring	Mirroring
mld	Multicast Listener Discovery Protocol
mvr	Multicast VLAN Registration
netlogin	Configure Network Login specific settings
ports	Port
radius	RADIUS Client
radius-accounting	RADIUS Client Accounting
rmon	RMON CLI command
sflow	Enable sFlow module
sharing	Sharing
smartredundancy	Smart redundancy on a port (software redundant port feature)
snmp	Configure SNMP specific settings
sntp-client	Enable SNTP client
stpd	STP domain
syslog	Configure syslog service
tacacs	TACACS+ client
tacacs-accounting	TACACS+ client accounting
tacacs-authorization	TACACS+ client CLI authorization
telnet	Allow incoming telnet connections
udp-echo-server	Enable a UDP-echo server
vlan	VLAN configuration
watchdog	Watchdog monitoring feature
web	WEB help
xml-cli	CLI-based XML configuration mode
xml-mode	Raw XML configuration mode
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<vlan-name>	VLAN name
exit	Exit configuration shell
history	Command history
install	Install system image
bootrom	Package to install

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
image	Package to install
load	Load system configuration
script	ExtremeXOS CLI script
logout	Exit configuration shell
ls	List file
internal-memory	Internal CF
mv	Rename file
internal-memory	Location is internal storage
<old-name>	Old file name
nslookup	Get IP address of host
<host-name-or-ip>	Host name or IP address
ping	Ping an IP address
continuous	Ping the specified host until stopped
count	Number of ping requests to send
dont-fragment	Set the IP do not fragment bit
interval	Time interval between sending out ping request
ipv4	Force use of IPv4 transport
ipv6	Force use of IPv6 transport
start-size	Start size of the ping packets to send
tos	Set the TOS value
ttl	Set the TTL value
udp	Use an UDP ping instead of ICMP ping
vr	Ping from specified virtual router
<host>	Host to ping
quit	Exit configuration shell
reboot	Reboot system
cancel	Cancel scheduled reboot
time	Scheduled reboot
refresh	Refresh system configuration
policy	Policy
reset	Reset
inline-power	Inline-power
restart	Restart device
ports	Ports
process	Process
rm	Remove file
internal-memory	File from internal storage
<file-name>	Name of the file to delete
rtlookup	Look up route to an IP address
<ipaddress>	Destination address
<ipv6address>	Destination address

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
run	Start new process
diagnostics	Perform diagnostics test
elrp	ELRP (Extreme Loop Recovery Protocol)
update	Read epmrc configuration file
save	Save system configuration
configuration	System configuration
primary	Primary configuration file
secondary	Secondary configuration file
show	Show running system information
access-list	Access list
accounts	Show accounts
banner	System login banner
bootprelay	Show the BOOTP relay information
checkpoint-data	Checkpoint data
configuration	System configuration
cpu-monitoring	CPU utilization statistics
debug	Debug information
dhcp-client	Show information related to dhcp-clients
dhcp-server	Show information related to the dhcp-server
diagnostics	Show diagnostic test results
diffserv	Diffserv
dns-client	Show configuration
dos-protect	Automatic denial-of-service protection
dot1p	Dot1p
dot1q	IEEE 802.1Q
eaps	EAPS (Ethernet Automatic Protection Switching)
edp	EDP information
elrp	ELRP (Extreme Loop Recovery Protocol)
elsm	ELSM (Extreme Link Status Monitoring)
esrp	ESR (Extreme Standby Router Protocol)
failsafe-account	Show the failsafe account information
fans	Fan information
fdb	FDB
forwarding	Show settings for hardware forwarding
heartbeat	Monitor process health
igmp	IGMP Protocol
inline-power	Inline-Power
ip-security	IP Security
iparp	IP ARP command
ipconfig	IP configuration
ipmroute	IP multicast routing module

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
iproute	IP routing module
ipstats	IP statistics
l2stats	Layer 2 statistics
lacp	LACP (Link Aggregation Control Protocol)
licenses	Switch licenses
lldp	Configure LLDP specific settings
log	Show information related to logging
mac-lockdown-timeout	MAC lockdown with timeout
management	Management
memory	Memory statistics
meter	METER help
mirroring	Mirroring
mld	MLDP
mvr	Multicast VLAN registration
neighbor-discovery	IPv6 neighbor
netlogin	Show network login specific information
odometers	Odometers
policy	Policy
ports	Ports
power	Power information
process	Process information
protocol	Protocol
qosprofile	QoS profile
radius	RADIUS and RADIUS accounting configuration
radius-accounting	RADIUS client accounting
rmon	RMON CLI command
session	Show active sessions
sflow	Show sFlow configuration
snmpv3	SNMPv3
sntp-client	Show configuration and statistics
ssl	SSL setup
stpd	STP domain
switch	Switch information
tacacs	TACACS+ configuration
tacacs-accounting	TACACS+ client accounting
tech	Technical support information
temperature	Temperature
tunnel	Tunnel
udp-echo-server	Show the UDP-echo server configuration
version	Version information
vlan	VLAN

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
vman	vMAN
<eapsDomain>	EAPS domain name
<name>	ESRP domain name
<stpd_name>	STP domain name
<vlan_name>	VLAN name
start	Start process
process	Process
telnet	Telnet client
vr	Virtual router
<host_name>	Remote host name
<remote_ip>	Remote telnet server IP address
terminate	Terminate running process
process	Process information
tftp	TFTP client
get	Get file
put	Put file
<host-name>	Remote TFTP server host name
<ip-address>	Remote TFTP server address
top	Display system utilization
traceroute	Trace route to an IP address
ipv4	Force use of IPv4 transport
ipv6	Force use of IPv6 transport
vr	Traceroute from virtual router ID
<host>	IPv4 host to traceroute
unconfigure	Unconfigure system configuration
access-list	Access list
bootprelay	BOOTP relay agent information option
diffserv	Diffserv
eaps	EAPS (Ethernet Automatic Protection Switching)
elrp-client	ELRP (Extreme Loop Recovery Protocol) Client
icmp	ICMP option
igmp	IGMP
inline-power	Inline-power
iparp	IP ARP command
lldp	Configure LLDP specific settings
log	Configure log service
mld	MLD protocol
mstp	MSTP configuration
netlogin	Configure network login specific settings
ports	Port
qosprofile	QoS profile

Table 29: Summit X150 and X350 Supported Commands (Continued)

Command	Description
radius	Unconfigure RADIUS server
radius-accounting	Unconfigure RADIUS accounting server
sflow	Unconfigure sFlow port
sntp-client	Unconfigure SNTP client
stpd	STP domain
switch	Switch configuration
tacacs	Unconfigure TACACS+ server
tacacs-accounting	Unconfigure TACACS+ accounting server
trusted-ports	Trusted ports
tunnel	Tunnel
vlan	VLAN
vman	vMAN
<eapsDomain>	EAPS domain name
<stpd_name>	STP domain name
<tunnel_name>	Tunnel name
<vlan_name>	VLAN name
uninstall	Uninstall system image
image	Package to uninstall
upload	Upload system configuration
configuration	System configuration
debug	Transfer support/debug data out of the switch
log	Show information related to logging
use	Select system configuration
configuration	System configuration
image	Package to run
vi	Invoke ExtremeXOS CLI editor
<filename>	ExtremeXOS CLI file name

Unsupported Commands on the Summit X150 and X350 Series Switches

Following is the list of processes that are not supported with an L2 Edge license.

- bgp
- msdp
- ospf
- ospfv3
- rip
- ripng
- pim

- vrrp
- brm
- upm

Table 30 lists the CLI commands not supported on the Summit X150 and X350 series switches.

Table 30: Summit X150 and X350 Unsupported Commands

Command	Description
configure	Configure running system information
ipforwarding	Configure IP forwarding behavior
ipmcforwarding	Configure IP multicast forwarding parameters
ipmroute	IP multicast routing module
irdp	ICMP Router Discovery Protocol
stacking	Settings for stacking
vlan {vlan_name} router-discovery	IPv6 router discovery
vlan {vlan_name} udp-profile	UDP forwarding profile
disable	Disable running system setting
esrp	ESRP (Extreme Standby Router Protocol) Domain
ipforwarding	IP forwarding
ipmcforwarding	IP multicast forwarding help
irdp	ICMP Router Discovery Protocol
router-discovery	IPv6 router discovery
stacking	Stacking
enable	Enable running system setting
esrp <esrp-domain>	ESRP (Extreme Standby Router Protocol) Domain
ipforwarding	IP forwarding
ipmcforwarding	IP multicast forwarding help
irdp	ICMP Router Discovery Protocol
router-discovery	IPv6 router discovery
stacking	Stacking
reboot	Reboot system
node-address	Reboot a node in the stack
stack-topology	Reboot stack-topology
show	Show running system information
router-discovery	IPv6 router discovery
stacking	Stacking information
udp-profile	UDP forwarding profile
synchronize	Synchronize entire primary MSM to backup MSM
stacking	Synchronize stacking configuration
unconfigure	Unconfigure system configuration
stacking	Settings for stacking
vlan {vlan_name} router-discovery	IPv6 router discovery
vlan {vlan_name} udp-profile	UDP forwarding profile

Tested Third-Party Products

This section lists the third-party products tested for ExtremeXOS 12.1.

Tested RADIUS Servers

The following RADIUS servers are fully tested:

- Microsoft—Internet Authentication Server
- Funk Software—Steel-Belted RADIUS Enterprise Edition 4.5
- Meetinghouse
- FreeRADIUS

Tested Third-Party Clients

The following third-party clients are fully tested:

- Funk Odyssey 2.2
- MeetingHouse Data AEGIS 2.0.5
- Odyssey 3.03.0.1194

PoE Capable VoIP Phones

The following PoE capable VoIP phones are fully tested:

- Avaya 4620
- Avaya 4620SW IP telephone
- Avaya 9620
- Avaya 4602
- Avaya 9630
- Avaya 4621SW
- Avaya 4610
- Avaya 1616
- Avaya one-X
- Cisco 7970
- Cisco 7910
- Cisco 7960
- ShoreTel ShorePhone IP 212k
- ShoreTel ShorePhone IP 560
- ShoreTel ShorePhone IP 560g
- ShoreTel ShorePhone IP 8000
- ShoreTel ShorePhone IP BB 24
- Siemens OptiPoint 410 standard–2

- Siemens OpenStage 20
- Siemens OpenStage 40
- Siemens OpenStage 60
- Siemens OpenStage 80

Extreme Switch Security Assessment

DoS Attack Assessment

Tools used to assess DoS attack vulnerability:

- Network Mapper (NMAP)

ICMP Attack Assessment

Tools used to assess ICMP attack vulnerability:

- SSPing
- Twinge
- Nuke
- WinFreeze

Port Scan Assessment

Tools used to assess port scan assessment:

- Nessus

2 Upgrading to ExtremeXOS 12.1

This chapter contains the following sections:

- Staying Current on page 97
- Upgrading ExtremeXOS on page 97
- Installing an ExtremeXOS Module on page 110
- Uninstalling an SSH Module on page 111
- Downgrading Switches on page 111

Staying Current

If you are an Extreme Assist customer, the latest release and release notes are available after logging in to the Tech Support web site at

http://www.extremenetworks.com/go/esupport.htm.

For more information about ExtremeXOS, see the *ExtremeXOS Concepts Guide* and the *ExtremeXOS Command Reference Guide*.

Upgrading ExtremeXOS

Upgrading your current ExtremeXOS installation to ExtremeXOS version 12.1 is a multistep process. In this section is a quick summary of the necessary steps, followed by detailed instructions.

NOTE

Hitless upgrade from ExtremeXOS 12.0 and earlier to ExtremeXOS 12.1 and later is not supported on the BlackDiamond 12800 switch.

NOTE

Hitless upgrade for network login is not supported when upgrading from an earlier version of ExtremeXOS software to ExtremeXOS 12.1 or later. If a hitless upgrade is required, you must globally disable network login and re-enable it when the upgrade is complete.

NOTE

See the "Hitless Upgrade Caveats for BlackDiamond 8800 Series Switches Only" in the ExtremeXOS Concepts Guide for an important caution about performing an MSM failover.

NOTE

Beginning with ExtremeXOS 12.1, an ExtremeXOS core image (.xos file) must be downloaded and installed on the alternate (non-active) partition. If you try to download to an active partition, the error message "Error: Image can only be installed to the non-active partition." is displayed. An ExtremeXOS modular software package (.xmod file) can still be downloaded and installed on either the active or alternate partition.

NOTE

With ExtremeXOS 12.1.3, the BlackDiamond 8800 series switches and the BlackDiamond 12800 series switches now require a firmware upgrade along with the standard software upgrade.

NOTE

A "Failed to install image" error occurs when trying to upgrade from ExtremeXOS 11.2.1 images to ExtremeXOS 11.6 or later. To upgrade to ExtremeXOS 12.1, you must currently be running ExtremeXOS 11.6 or later. If you are not running 11.6 or later you must first upgrade to ExtremeXOS 11.6 and then upgrade to ExtremeXOS 12.1.

Quick Summary

To install and upgrade to ExtremeXOS 12.1 on your system, you will be following these steps:

1. Download the image to your TFTP server.
2. Verify which virtual router connects to your TFTP server.
3. Save your configuration to a backup configuration file.
4. Determine your selected and booted image partitions.
5. Select the download partition and partition to use on reboot.
6. Download and install the image to the switch.
7. Reboot the switch.
8. Save the configuration for the new image.
9. Upgrade the BootROM—BlackDiamond 10808 switch only.
10. Upgrade the BootROM and PSU controller firmware--BlackDiamond 8800 family of switches only.
11. Upgrade the BootROM and PSU controller firmware--BlackDiamond 12804 family of switches only.

NOTE

If you have a dual MSM system, and the software image is not the same on both MSMs, see the section "Dual MSM Systems with Different Images Present" on page 108.

Detailed Steps

NOTE

Extreme Networks recommends using a TFTP server that supports blocksize negotiation (per RFC-2348). Using this type of server enables the switch to download the images faster.

To upgrade to ExtremeXOS 12.1 on your system, follow these steps:

1 Download the image to your TFTP server.

Download the image you received from Extreme Networks to your TFTP server.

2 Verify which virtual router connects to your TFTP server.

Use the following `ping` commands to test which virtual router you will need to specify when you download the image to your switch. This example assumes that your TFTP server's IP address is 192.168.0.12; substitute your own address when you run the command:

```
ping vr vr-mgmt 192.168.0.12
ping vr vr-default 192.168.0.12
```

At least one of these commands must successfully reach your TFTP server for you to download the image. When you download the image in step 6, specify the virtual router that allowed you to reach your TFTP server.

3 Save your configuration to a backup configuration file.

You must save your configuration to a backup configuration file, or you will be unable to revert to your currently running image, if the need arises. In this example, we use the software version number as part of the name. Use the following command to save the configuration to the file *version11_6_1_7.cfg*:

```
save configuration version11_6_1_7
```

As an optional, extra precaution, we suggest that you save this configuration to a TFTP server. Use the `tftp` command to save your configuration. In the following example, the TFTP server's IP address is *192.168.0.12*, the virtual router determined in step 2 is *vr-mgmt*, and the configuration file is *version11_6_1_7.cfg*:

```
tftp 192.168.0.12 -v vr-mgmt -p -l version11_6_1_7.cfg
```

4 Determine your selected and booted image partitions.

Run the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the primary partition.

```
...
Image Selected:      primary
Image Booted:        primary
Primary ver:         11.6.1.7
Secondary ver:       11.6.1.7

Config Selected:     primary.cfg
Config Booted:       primary.cfg
```

5 Select the download partition and partition to use on reboot.

Specify the partition by issuing the following command:

```
use image pri
```

OR

```
use image sec
```

6 Download and install the image to the switch.

Download and install the image to the switch using the `download image` command. The virtual router `<vr>` that you will use is the one you determined in step 2. This example assumes that you are using virtual router *vr-mgmt* and TFTP server *192.168.0.12*. Substitute your own virtual router and IP address when you run the command:

```
download image 192.168.0.12 bd10k-12.1.3.xos vr vr-mgmt
```

(This may not be the actual filename; it is just an example.)

You will be asked:

```
Do you want to install image after downloading ? (y—yes, n—no, <cr>—cancel)
```

Answer *y*, for yes, so that the image will be installed after downloading.

7 Reboot the switch.

Use the `reboot` command to reboot the switch.

NOTE

For the BlackDiamond 8800 series of switches—You will be prompted to upgrade the BootROM on the BlackDiamond 8800 series of switches when installing the ExtremeXOS image. If you answer "y" for yes after the prompt and install the image after downloading, you will also be prompted to install the new BootROM during the installation process before the switch reboots.

8 Save the configuration for the new image.

Even though your configuration was saved before you rebooted, you will need to save the configuration with the new image. If you wait to login for some time after the reboot, you will receive a notice that recommends that you save the configuration. If you login soon after the reboot, you will not receive the notice, although an asterisk (*) will appear before the command prompt, indicating that the current configuration is not saved. In either case, save the configuration with the command:

```
save configuration
```

9 Upgrade the BootROM—BlackDiamond 10808 switch only.

Extreme Networks recommends that you upgrade to the latest BootROM for the BlackDiamond 10808. While not strictly required for this release, it is highly recommended. Run the `show version` command to verify the BootROM version currently running on your switch. If you are not running BootROM version 1.0.1.5 or later, upgrade the BootROM using the following command:

```
download bootrom 192.168.0.12 bd10k-1.0.1.5-bootrom.xbr
```

This example assumes that you will use the same TFTP server and virtual router as in step 6 above.

You will be asked if you want to install the BootROM after downloading. Answer yes, or use the `install bootrom` command to install later. Once the BootROM is downloaded and installed, it replaces the previous image stored in the onboard FLASH memory, and will be used at the next reboot.

10 Upgrade the BootROM and PSU controller firmware--BlackDiamond 8800 family of switches only.

NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 8800 series of switches with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM BootROM	1.0.3.7	First available in ExtremeXOS 12.1.1.4
I/O module BootROM	1.0.3.7	First available in ExtremeXOS 12.1.1.4
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the new BootROMs or firmware only on modules that have older BootROMs or firmware installed. You will be asked if you want to install each type of BootROM or firmware. New PSU controller firmware is used immediately after it is installed without rebooting the switch. The new BootROM and firmware overwrite the older versions stored in FLASH memory.

```
BD-8806.2 # install firmware
Installing version 1.0.1.11 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Do you want to save configuration changes to primary.cfg? (y or n) Yes
Saving configuration on primary MSM ....... done!
Installing version 1.0.1.11 of the IO module bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes

Installing bootrom...

MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...

IO module bootrom(s) installed successfully
IO module bootrom(s) will be activated upon next IO module reboot

Installing firmware...
PSU controller firmware installed successfully
BD-8806.3 #
```

11 Upgrade the BootROM and PSU controller firmware--BlackDiamond 12804 family of switches only.

NOTE

BootROMs installed by Manufacturing should never be forced to an earlier BootROM version unless explicitly instructed by Extreme Networks support.

Extreme Networks requires that you upgrade the MSMs, I/O modules, and PSU controllers in the BlackDiamond 12804 with the BootROM and firmware images included in this release of ExtremeXOS.

This release of ExtremeXOS contains the following versions of the BootROM and firmware:

MSM Bootloader	1.0.0.3	First available in ExtremeXOS 11.4.1.4
PSU controller firmware	2.13	First available in ExtremeXOS 11.4.1.4

Use the `show version` command to display the versions of the BootROM and firmware currently installed.

NOTE

For single MSM systems, reboot the switch using the `reboot` *command after the firmware installation is complete.*

To install the new BootROM and firmware, wait until the `show slot` command indicates the MSMs and I/O modules are operational. Then use the `install firmware` command. This command will install the BootROMs and/or firmware only on modules that have older BootROMs or firmware installed. Once this installation is complete, reboot the switch using the `reboot` command.

NOTE

For dual MSM systems, the `install firmware` *command cannot install all the necessary software while the MSM is primary. To completely install the firmware, an MSM failover is required. First, run the* `install firmware` *command on the primary MSM. When the installation is complete, run the* `run msm-failover` *command to allow the switch to failover to the secondary MSM. Run the* `install firmware` *command on the new primary MSM. To revert back to your original primary MSM, run the* `run msm-failover` *command. Because two failovers are required for a dual-MSM firmware installation, you* ***will not*** *need to run the* `reboot` *command after executing the* `install firmware` *procedure.*

NOTE

Upgrading a BlackDiamond 12804 slot can take a minimum of six minutes per slot.

```
BD-12804.7 # install firmware
Installing version 1.0.0.2 of the MSM bootrom(s). Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing IO module firmware, a reboot is required. Do you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing version 2.13 of the PSU control module firmware. Do you want to
continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing micro controller image on backup MSM requires rebooting backup MSM. Do
you want to continue?
(y - yes, n - no, <cr> - cancel) Yes
Installing bootrom...
Installing bootstrap
Installing active bootrom
Installing system FPGA image
Installing bootstrap
Installing active bootrom
Installing system FPGA image

MSM bootrom(s) installed successfully
MSM bootrom(s) will be activated upon next MSM reboot
Installing bootrom...
```

```
Installing microcontroller firmware to slot 1 ...
Installing FGPA firmware to slot 1. This will takes a few minutes...
Installing microcontroller firmware to slot 2 ...
Installing FGPA firmware to slot 2. This will takes a few minutes...
Installing microcontroller firmware to slot 5 ...
Installing FGPA firmware to slot 5. This will takes a few minutes...
Installing microcontroller firmware to slot 6 ...
Installing FGPA firmware to slot 6. This will takes a few minutes...
```

To verify that your firmware upgrade on both the MSM and I/O modules has been successful, verify using the following command:

```
show version detail
```

```
BD-12804.1 # show version detail
```

```
Chassis    : 804030-00-05 07085-00026 Rev 5.0
Slot-1     : 804031-00-05 0706F-00200 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-2     : 804031-00-05 0703F-00184 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-5     : 804031-00-05 0703F-00185 Rev 5.0 uC: 5.00 FPGA: 5.0d
Slot-6     :
MSM-A : 804046-00-07 0706F-00117 Rev 7.0 BootROM: 1.0.0.3 IMG: 12.1.3   uC: 5.00
FPGA: 3.30
MSM-B      : 804046-00-07 0706F-00122 Rev 7.0 BootROM: 1.0.0.3     IMG: 12.1.4
uC: 5.00
PSUCTRL-1 : 700111-00-01 06525-00997 Rev 1.0 BootROM: 2.13
PSUCTRL-2 : 700111-00-01 06525-00909 Rev 1.0 BootROM: 2.13
PSU-1      : PS 2336 4300-00145 0641K-22897 Rev 1.0
PSU-2      : PS 2336 4300-00145 0641K-23307 Rev 1.0
PSU-3      : PS 2336 4300-00145 0641K-23266 Rev 1.0
PSU-4      :
PSU-5      :
PSU-6      :
Image    : ExtremeXOS version 12.1.4 v1202b25 by release-manager
on Tue Nov 6 22:56:10 PST 2007
BootROM : 1.0.0.3
BD-12804.2 #
```

Following is an example of the old FPGA version:

```
MSM =  3.2a
I/O = 5.07 or earlier
```

Following is an example of the new FPGA version:

```
MSM= 3.30
I/O = 5.0d
```

The backup MSM version is not shown until the MSM is made the primary MSM.

Upgrading ExtremeXOS on a Summit X150 and X350

Upgrade ExtremeXOS on a Summit X150 and X350 to ExtremeXOS 12.1.4 as follows:

1. Save your configuration to a backup configuration file using the `save configuration <configuration_file_name>` command.

   You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2. Run the `show version` command to verify the BootROM version currently running on your switch.

If you are not running BootROM version 1.0.3.1, upgrade the BootROM using the following command:

```
download bootrom <tftp server ipaddress> pmon_summit-1.0.3.1.xtr vr <vrname>
```

3 Determine your current active image partition by running the `show switch` command. The Image Booted field shows the current active partition.

4 Download the ExtremeXOS 12.1.4 image to the alternate partition using the following command:

```
download image <ipaddress> <filename> vr <vrname> <image partition>
```

For example, if your current image is running in the primary partition, download the new image in the secondary partition:

```
download image 10.60.116.11 summitX-12.1.4.xos vr vr-mgmt secondary
```

5 Run the `show switch` command again to determine that the image is downloaded into the partition you have specified.

6 Reboot the switch.

Use the `reboot` command to reboot the switch.

7 When the switch comes up, run the `save configuration` command to save the configuration in the upgraded image.

Upgrading ExtremeXOS on a Summit X250e

Upgrade a Summit X250e to ExtremeXOS 12.1.4 as follows:

1 Save your configuration to a backup configuration file using the `save configuration <configuration_file_name>` command.

You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2 Run the `show version` command to verify the BootROM version currently running on your switch. If you are not running BootROM version 1.0.3.0, upgrade the BootROM using the following command:

```
download bootrom 10.60.116.11 pmon_Combined_1_0_3_0.xtr vr vr-mgmt
```

3 Determine your current active image partition by running the `show switch` command. The Image Booted field shows the current active partition.

4 Download the ExtremeXOS 12.1.4 image to the alternate partition using the following command:

```
download image <ipaddress> <filename> vr <vrname> <image partition>
```

For example, if your current image is running in the primary partition, download the new image in the secondary partition:

```
download image 10.60.116.11 summitX-12.1.4.xos vr vr-mgmt secondary
```

5 Run the `show switch` command again to determine that the image is downloaded into the partition you have specified.

6 Reboot the switch.

Use the `reboot` command to reboot the switch.

7 When the switch comes up, run the `save configuration` command to save the configuration in the upgraded image.

Upgrading ExtremeXOS on a Summit X450

Upgrade a Summit X450 to ExtremeXOS 12.1.4 as follows:

1 Save your configuration to a backup configuration file using the `save configuration` command.

You must save your configuration to a backup configuration file in order to revert to your currently running image if the need arises.

2 Download the latest image to the switch.

Download the image to the switch using the `download image` command. Download ExtremeXOS 12.1 image `summitX-12.1.4.xos`.

3 Determine your current active image partition by running the `show switch` command. The Image Booted field shows the current active partition.

4 Download the ExtremeXOS 12.1.4 image to the alternate partition using the following command:

```
download image <ipaddress> <filename> vr <vrname> <image partition>
```

For example, if your current image is running in the primary partition, download the new image in the secondary partition:

```
download image 10.60.116.11 summitX-12.1.4.xos vr vr-mgmt secondary
```

5 Reboot the switch.

Use the `reboot` command to reboot the switch.

Upgrading an MSM-5 and MSM-5R to ExtremeXOS 12.1 on a BlackDiamond 12802

Upgrade the MSM-5 or MSM-5R to ExtremeXOS 12.1.4 as follows:

1 From the Extreme Networks eSupport website, download the ExtremeXOS 12.1.4 FCS image to your TFTP server.

When powered up, the BlackDiamond 12802 comes up as a BlackDiamond 12804. An error is displayed on the console and in the logs similar to the following:

```
Running Image ...

ohdGetChassisInfo: Incorrect Chassis type found, defaulting to BIATHLON
ohd_init_hw: Error determining chassis info
Starting Extremeware XOS 11.4.3b4
Copyright (C) 1996-2006 Extreme Networks.  All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388; 6,034,957;
6,859,438; 6,912,592; 6,954,436.

Error: Failed to connect CLI for 16 seconds!
login: admin
password:

ExtremeWare XOS
Copyright (C) 2000-2006 Extreme Networks. All rights reserved.
Protected by US Patent Nos: 6,678,248; 6,104,700; 6,766,482; 6,618,388; 6,034,957;
6,859,438; 6,912,592; 6,954,436.
```

```
========================================================================== BD-
12804.1 # show log
05/02/2007 00:27:10.81 <Info:HAL.Card.Info> MSM-A: Module in MSM-A is operational
05/02/2007 00:27:10.39 <Info:AAA.authPass> MSM-A: Login passed for user admin
through serial
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_read: Error reading
eeprom for slot 15 at offset 0
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_read: Error reading
eeprom for slot 15 at offset 0
05/02/2007 00:27:07.75 <Erro:Kern.Error> MSM-A: ohd_eeprom_access: Error accessing
device -1
```

2 Use the management VLAN virtual router to connect to your TFTP server by configuring an IP address on the management VLAN using the following command:

```
configure mgmt ipaddress 192.168.1.134/24
```

Enter a default gateway using the following command:

```
configure iproute add default 10.201.1.1 vr "VR-Mgmt"
```

NOTE

The default VLAN has no ports because it does not recognize the chassis.

3 Test which virtual router you will need to specify when you download the image to your switch by using the following command and your own IP address:

```
ping vr vr-mgmt 192.168.0.12
```

This command must successfully reach your TFTP server in order to download the image.

4 Download and install the image to the switch using the following command:

```
download image 192.168.0.12 bd12k-12.1.4.xos vr vr-mgmt
```

5 When the switch returns the following message:

```
Do you want to install image after downloading ? (y-yes, n-no, <cr>-cancel)
```

Answer "y" to install the image after downloading.

6 Use the `reboot` command to reboot the switch.

7 Run the `show switch` command. Verify that the `SysName` and `System Type` read `BD-12802`, and that the image is specified as `12.1.4`.

```
SysName:          BD-12802
SysLocation:
SysContact:       support@extremenetworks.com, +1 888 257 3000
System MAC:       00:04:96:31:A2:40
System Type:      BD-12802

SysHealth check:  Enabled (Normal)
Recovery Mode:    All
System Watchdog:  Enabled

Current Time:     Thu May  3 11:31:07 2007
Timezone:         [Auto DST Disabled] GMT Offset: 0 minutes, name is UTC.
Boot Time:        Thu May  3 11:26:38 2007
Boot Count:       11
Next Reboot:      None scheduled
System UpTime:    4 minutes 29 seconds
```

```
Slot:              MSM-A *
                   ------------------------
Current State:     MASTER

Image Selected:    secondary
Image Booted:      secondary
Primary ver:       12.0.0.13
Secondary ver:     12.1.2

Config Selected:   NONE
Config Booted:     Factory Default
```

Upgrading a BlackDiamond Series of Switches Using Hitless Upgrade

NOTE

You must be running ExtremeXOS 11.1.1.9 or later to use hitless upgrade on a BlackDiamond 10808 switch.

NOTE

For the BlackDiamond 8800 series of switches, a hitless upgrade to ExtremeXOS 12.1.1 from an earlier release is not supported. Use the normal software upgrade process for these switches.

Upgrading the Alternate Partition Using Hitless Upgrade

Performing a hitless upgrade on the alternate partition allows you to revert to the previous image in case the upgrade is not successful. Upgrade the alternate partition using hitless upgrade as follows:

1 Run the `show switch` command to determine which partition is the active partition and which partition is the alternate partition.

2 In the following example, the secondary image is the active partition. The download is performed on the primary image.

Execute the CLI command `download image 10.201.14.13 bd12k-12.1.4.xos primary`

```
* BD-12804.8 # download image 10.201.13.14 bd12k-12.1.4.xos primary
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
Yes
```

3 When the download is complete, run the `show switch` command to confirm the new image downloaded to the primary image.

4 Verify the following before rebooting the backup MSM:

- "Primary ver:" is the image to be downloaded.
- "Image Selected" is set to primary.

```
MSM:                MSM-A *           MSM-B
                    ------------------------------------
Current State:      MASTER            BACKUP (In Sync)
Image Selected:     primary           primary
Image Booted:       secondary         secondary
```

```
Primary ver:          12.1.2              12.1.2
Secondary ver:        11.4.1.4            11.4.1.4
```

5 Run the `reboot` command to reboot MSM-B only.

```
reboot msm b
```

6 Run the `show switch` command to verify that:

- MSM-B is (In Sync) mode.
- "Image Selected" and "Image Booted" are both set for primary on the backup MSM.

```
MSM:                  MSM-A *             MSM-B
                      ------------------------------------

Current State:        MASTER              BACKUP (In Sync)
Image Selected:       primary             primary
Image Booted:         secondary           primary
Primary ver:          12.1.2              12.1.2
Secondary ver:        11.4.1.4            11.4.1.4
```

7 Execute the `run msm-failover` command from the master MSM (MSM-A).

8 MSM-B becomes the master MSM, and MSM-A will reboot.

9 Run the `show switch` command to:.

- Verify that MSM-B is the master MSM and MSM-A is the backup MSM and displays (In Sync).
- Verify that "Image Selected" and "Image Booted" are set for primary on both MSMs.

```
MSM:                  MSM-A               MSM-B *
                      ------------------------------------

Current State:        BACKUP (In Sync)    MASTER
Image Selected:       primary             primary
Image Booted:         primary             primary
```

10 Run the `run msm-failover` command again so that MSM-A becomes the master MSM.

11 Run the `show switch` command to confirm the master MSM is now MSM-A.

```
MSM:                  MSM-A *             MSM-B
                      ------------------------------------

Current State:        MASTER              BACKUP (In Sync)
Image Selected:       primary             primary
Image Booted:         primary             primary
Primary ver:          12.1.2              12.1.2
Secondary ver:        11.4.1.4            11.4.1.4
```

Dual MSM Systems with Different Images Present

If you have a dual MSM system that has different images on the MSMs, you will need to modify the upgrade procedure. One situation where you might have different images installed is when you add an MSM that has been in storage to your chassis, either for the first time, or as a replacement. You will only need to do the following procedure if one of the MSMs is running an image earlier than 11.0.0, and the images are different on the two MSMs (earlier versions of the software are unable to automatically synch up the configurations).

Follow the directions for upgrading the switch, and continue with step 6. When you download the image, as described in step 6, Download and install the image to the switch., you will be asked:

```
Do you want to install image after downloading ? (y—yes, n—no, <cr>—cancel)
```

Answer *n*, for no, so that the image will not be installed after downloading.

Next, manually install the image, using the following command:

```
install image bd10k-12.1.4.xos
```

Now the two MSMs have the same image installed, but may not have the same configurations. Reboot the secondary MSM using one of the following commands:

`reboot msm b` (if you are running on MSM A)

`reboot msm a` (if you are running on MSM B)

Finally, save the configuration on both MSMs by using the command

```
save configuration
```

Using a Rev 10 (or later) BlackDiamond 10808 MSM-1 or MSM-1XL

NOTE

To use a Rev 10 (or later) MSM-1 or MSM-1XL module, you must upgrade both the active and alternate images with the latest ExtremeWare 11.1.3 (or later) software image.

To determine which version of MSM you have installed in your switch, use the `show version` command.

If you have a Rev 9 (or earlier) MSM, the `show version` command output will look like this:

```
MSM-A :804015-00-09 0414F-00728 Rev 9.0 BootROM: 1.0.1.5 IMG:
```

If you have a Rev 10 (or later) MSM, the `show version` command output will look like this:

```
MSM-A :804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
```

Complete `show version` command output with Rev 10 MSMs will look like this:

```
BD-10808.2 #
BD-10808.2 # show version
Chassis    : 804300-00-03 0324X-00026 Rev 3.0
MSM-A      : 804407-00-10 0505F-00429 Rev 10.0 BootROM: 1.0.1.5 IMG:
MSM-B      : 804407-00-10 0505F-00431 Rev 10.0 BootROM: 1.0.1.5 IMG:
Image    : ExtremeXOS version 11.1.3.3 v11133 by release-manager on Thu Mar 31
19:12:57 PST 2005
BootROM : 1.0.1.7
BD-10808.3 #
```

Installing an ExtremeXOS Module

An ExtremeXOS module has functionality that supplements a core image. You will download and install a module onto an already installed core image. The version number of the core image and the module must match. For example, the module *bd10k-12.1.4-ssh.xmod* can only be installed onto the core image *bd10k-12.1.4.xos*.

You can download and install the SSH module.

NOTE

You must terminate and restart the thttpd process before you can use SSL.

Assuming that you have an installed and running ExtremeXOS 12.1 software on the active partition, follow these steps to install the module:

1 Download the module image to your TFTP server.

Download the image you received from Extreme Networks to your TFTP server.

2 Determine the active partition for your switch.

Run the `show switch` command to determine your current selected and booted image partitions. The booted image partition indicates the currently active partition.

3 Download and install the module image to the active partition.

Download the image to the switch using the `download image` command. The `filename` for the only available module image is *bd10k-12.1.4-ssh.xmod*.

The virtual router `<vr>` that you will use is the one that connects to your TFTP server (you determined this in step 2, "Verify which virtual router connects to your TFTP server." in the upgrade procedure). Since the system virtual router names changed from release 10.1.2.17 to 11.2.3.3, the name will be different from that used to download the initial upgrade image. Use *vr-mgmt* for this step or *vr-default*.

This example assumes that you are using virtual router *vr-mgmt* and TFTP server *192.168.0.12*, substitute your own virtual router and IP address when you run the command:

```
download image 192.168.0.12 bd10k-12.1.4-ssh.xmod vr vr-mgmt <partition> (primary
or secondary)
```

You will be asked:

```
Do you want to install image after downloading? (y - yes, n - no, <cr> - cancel)
```

Answer *y*, for yes, so that the image will be installed after downloading.

4 Run the `run update` command.

Run the following command:

```
run update
```

The `run update` command starts up the processes associated with the new module, and makes them available to the system. You should now be able to run the commands associated with SSH2.

You can verify that the SSH2 module is running by issuing the following command:

```
show process
```

If SSH2 is running, you will see a process named *exsshd* listed. You can then configure and enable SSH2 on the switch.

You can also verify that the SSH2 module is installed by issuing the following command:

```
show management
```

If the SSH module is installed, you will see text similar to the following:

```
SSH access : Disabled (Key invalid, tcp port 22 vr all)
```

If the SSH module is not installed, you will see text similar to the following:

```
SSH Access : ssh module not loaded.
```

Uninstalling an SSH Module

To uninstall the SSH module you must first terminate the THTTPD process:

1. Run the `terminate process thttpd graceful` command. This terminates the THTTPD process.
2. Run the `uninstall image bd10k-12.1.4-ssh.xmod` <partition> (`primary or secondary`) command. This uninstalls SSH from your switch.
3. Restart the thttpd process using the `start process thttpd` command.

Downgrading Switches

Following are the instructions for downgrading your ExtremeXOS version 12.1.4 installation to a previous version. It is assumed that you saved your configuration using the 11.4.1 image, and that the 11.4.1 image is currently installed on the switch, on the non-booted partition.

NOTE

Do not downgrade a BlackDiamond 8810 switch to an image earlier than 11.1.1 or a Summit X450 switch to an image earlier than 11.2.1. Do not downgrade a BlackDiamond 8806 switch to an image earlier than 11.3.1.3. Do not downgrade a Summit X450a or X450e switch to an ExtremeXOS image earlier than 11.5.1.

To downgrade to the existing ExtremeXOS version 11.4.1 image on your system, you will be following these steps:

1. Determine your selected and booted image partitions.

   Run the `show switch` command to determine your current selected and booted image partitions. The selected image partition indicates which image will be used at the next reboot. The booted image partition indicates which image was used at the last reboot.

   Output from this command includes the version of the selected and booted images and if they are in the primary or the secondary partition. In this example, the selected and booted images are in the secondary partition.

```
...
Image Selected:     secondary
Image Booted:       secondary
Primary ver:        11.4.1.4
Secondary ver:      12.1.2

Config Selected:    primary.cfg
Config Booted:      primary.cfg
```

2 Select the reboot partition.

Assuming that the 11.4.1 image is on the non-booted partition, if you are currently running the image booted from the primary partition, run this command:

```
use image secondary
```

If you are currently running the image booted from the secondary partition, run this command:

```
use image primary
```

3 Select the reboot configuration.

Select the configuration to be used after reboot with the `use configuration` command. Assuming you saved the 11.4.1 configuration as *bdversion11_4_1_4.cfg*, use the following command:

```
use configuration bdversion11_4_1_4
```

4 Verify the image and configuration selection.

Again, run the `show switch` command. The output should show that the selected image is the 11.4.1 image that you are downgrading to, and the selected configuration is the one you saved before you installed the 12.1.4 image:

```
...
Image Selected:   primary
Image Booted:     secondary
Primary ver:      11.4.1.4
Secondary ver:    12.1.3.14

Config Selected:  bdversion11_4_1_4.cfg
Config Booted:    primary.cfg
...
```

5 Reboot the switch.

Use the command `reboot` to reboot the switch.

3 Limits

This chapter summarizes the supported limits in ExtremeXOS 12.1.4.

Supported Limits

Table 31 summarizes tested metrics for a variety of features, as measured in a per-system basis unless otherwise noted. These limits may change but represent the current status. The contents of this table supersede any values mentioned in the *ExtremeXOS Concepts Guide*.

NOTE

The scaling and performance information shown in Table 31 is provided for the purpose of assisting with network design. It is recommended that network architects and administrators design and manage networks with an appropriate level of network scaling "head room." The scaling and performance figures provided have been verified using specific network topologies using limited switch configurations. There is no guarantee that the scaling and performance figures shown are applicable to all network topologies and switch configurations and are provided as a realistic estimation only. If you experience scaling and performance characteristics that you feel are sufficiently below what has been documented, contact Extreme Networks technical support for additional assistance.

NOTE

The route limits shown in Table 31 for IPv4 and IPv6 routing protocols are software limits only. The actual hardware limits may be lower than the software limits, based on platform. The hardware limits for specific platforms are specified as "IPv4/IPv6 routes (LPM entries in hardware)" in the following table.

NOTE

On a BlackDiamond 8800 or a Summit X450 or X250e switch, it is not advised to have greater than 25,000 total IP routes from all routing protocols. Adverse effects can occur with routing tables larger than this, especially when a single network event or CLI command affects a significant number of routes. For example, just after such a network event, the added system load will cause a "save configuration" command to time out.

Table 31: Supported Limits

Metric	Product	Limit
Access lists (masks)—maximum number of ACL masks per port.[a]	BlackDiamond 8800 original series	16
	Summit X450	16
Access lists (policies)—suggested maximum number of lines in a single policy file.	BlackDiamond 10808	300,000
	BlackDiamond 12800 series	300,000

Metric	Product	Limit
Access lists (policies)—maximum number of rules in a single policy file.[b]	BlackDiamond 8800 series	
	Original series modules (per GigE port) (per 10 GigE port)	128 1,016
	c-series modules	4,096
	a-series modules	2,048
	e-series modules	1,024
	BlackDiamond 10808	30,000
	Summit X150 and X350 series	1,024
	Summit X250e	
	per port groups 1-24 and 25-48	1,024
	Summit X450	
	(per GigE port) (per 10 GigE port)	128 1,016
	Summit X450a	
	per port groups 1-24 and 25-48	2,048
	Summit X450e	
	per port groups 1-24 and 25-48	1,024
Access lists (slices)—maximum number of field selectors for ACL slices.	BlackDiamond 8800 series	
	c-series and a-series modules per port groups 1-12, 25-36 and 13-24, 37-48	16
	e-series modules per port groups 1-12, 25-36 and 13-24, 37-48	8
	Summit X150 and X350 series	8
	Summit X250e	
	per port groups 1-24 and 25-48	8
	Summit X450a	
	per port groups 1-24 and 25-48	16
	Summit X450e	
	per port groups 1-25	8
AAA (local)—maximum number of admin and local user accounts.	All platforms	16
BGP (aggregates)—maximum number of BGP aggregates.	All platforms with Core license or above	256
BGP (networks)—maximum number of BGP networks.	All platforms with Core license or above	1,024

Metric	Product	Limit
BGP (peers)—maximum number of BGP peers.	BlackDiamond 8800 series	256*
	BlackDiamond 10808	
	MSM-1XL	512
	MSM-1	256
	BlackDiamond 12800 series	
	MSM-5	256
	MSM-5R	256*
	MSM-6R	512
	Summit X450	128*
	Summit X450a	128*
	* With default keepalive and hold timers.	
BGP (peer groups)—maximum number of BGP peer groups.	All platforms with Core license or above	64
BGP (policy entries)—maximum number of BGP policy entries per route policy.	All platforms with Core license or above	256
BGP (policy statements)—maximum number of BGP policy statements per route policy.	All platforms with Core license or above	1,024
BGP (unicast address-family routes)—maximum number of unicast address-family routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series	25,000
	BlackDiamond 10808	
	MSM-1XL	1,000,000
	MSM-1	400,000
	BlackDiamond 12800 series	
	MSM-5	400,000
	MSM-5R	400,000
	MSM-6R	1,000,000
	Summit X450	25,000
	Summit X450a	25,000
BGP (non-unique routes)—maximum number of non-unique BGP routes (LPM entries is limited to support TCAM entries on a BlackDiamond 10808).	BlackDiamond 8800 series	25,000
	BlackDiamond 10808	
	MSM-1XL	2,000,000
	MSM-1	900,000
	BlackDiamond 12800 series	
	MSM-5	900,000
	MSM-5R	900,000
	MSM-6R	2,000,000
	Summit X450	25,000
	Summit X450a	25,000
BGP multicast address-family routes —maximum number of multicast address-family routes.	BlackDiamond 8800 series	25,000
	BlackDiamond 10808	
	MSM-1XL	1,000,000
	MSM-1	450,000
	BlackDiamond 12800 series	
	MSM-5	450,000
	MSM-5R	450,000
	MSM-6R	1,000,000
	Summit X450	25,000
	Summit X450a	25,000

Metric	Product	Limit
BOOTP/DHCP relay—maximum number of BOOTP or DHCP servers per virtual router.	All platforms	4
CLEAR-Flow—total number of rules supported. The ACL rules plus CLEAR-Flow rules must be less than the total number of supported ACLs. **Note:** CLEAR-Flow is not supported on "e" series switches and is only supported in a non-stack configuration in the Summit family of switches.	BlackDiamond 8800 c-series Summit X450a	4,096 2,048
Connectivity Fault Management (CFM)—maximum number or CFM domains.	All platforms	8
CFM—maximum number of CFM associations.	All platforms	4,094
CFM—maximum number of CFM up end points.	All platforms	32
CFM—maximum number of CFM down end points.	All platforms	32
CFM—maximum number of CFM remote end points.	All platforms	64
CFM—maximum number of dot1ag ports.	All platforms	128
Dynamic ACLs—maximum number of ACLs processed per second. **Note**: Limits are load dependent.	BlackDiamond 8800 with c-series MSM and I/O modules BlackDiamond 12800 series Summit X450a with 50 DACLs with 500 DACLs	 8 12 10 5
EAPS domains—maximum number of EAPS domains. **Note**: An EAPS ring that is being spatially reused cannot have more than four configured EAPS domains.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit series	64 128 128 32
EAPSv1 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit series	2,000 4,000 4,000 1,000
EAPSv2 protected VLANs—maximum number of protected VLANs.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit series	1,000 4,000 4,000 500
ELSM (vlan-ports)—maximum number of VLAN-ports.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series	5,000 5,000 5,000
ESRP groups—maximum number of ESRP groups.	All platforms	7
ESRP domains—maximum number of ESRP domains.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit series	64 128 64 64

Metric	Product	Limit
ESRP VLANs—maximum number of ESRP VLANs.	BlackDiamond 8800 series	1,000
	BlackDiamond 10808	3,000
	BlackDiamond 12800 series	3,000
	Summit series	1,000
ESRP (maximum ping tracks)—maximum number of IP route tracks per VLAN.	All platforms	8
ESRP (IP route tracks)—maximum IP route tracks per VLAN.	All platforms	8
ESRP (VLAN tracks)—maximum number of VLAN tracks per VLAN.	All platforms	1
Forwarding rate—maximum L2/L3 software forwarding rate.	BlackDiamond 8800 series	10,000 pps
	BlackDiamond 12800 series	16,000
	Summit X250e	10,000 pps
	Summit X450	10,000 pps
FDB (blackhole entries)—maximum number of unicast blackhole FDB entries.	BlackDiamond 8800 original series	16,000
	BlackDiamond 8800 a-series	16,000
	BlackDiamond 8800 e-series	8,000
	Summit X450 original	16,000
	Summit X450a	16,000
	Summit X450e	8,000
FDB (blackhole entries)—maximum number of multicast blackhole FDB entries.	BlackDiamond 8800 original series	256
	BlackDiamond 8800 a-series	1,024
	BlackDiamond 8800 e-series	1,024
	Summit X450 original	256
	Summit X450a	1,024
	Summit X450e	1,024
FDB (maximum L2/L3 entries)—maximum number of MAC addresses/IP host routes.	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
FDB (maximum L2 entries)—maximum number of MAC addresses.	BlackDiamond 8800 original	16,384
	BlackDiamond 8800 c-series	32,768
	BlackDiamond 8800 a-series	16,384
	BlackDiamond 8800 e-series	8,192
	BlackDiamond 8800 (system)	128,000
	Summit X150 and X350 series	8,192
	Summit X250e	8,192
	Summit X450	16,384
	Summit X450a	16,384
	Summit X450e	8,192
	SummitStack™	128,000

Metric	Product	Limit
Hierarchical QoS—maximum number of ingress-only traffic queues per system. (For 20XTR, first 10 ports ranges from 1 to 10 are UNIT-I, second 10 ports ranges from 11 to 20 are UNIT-II, for 10 Gig slot each port is one UNIT.)	BlackDiamond 12800 R-series	4,076
Hierarchical QoS—maximum number of ingress traffic queues with egress shaping allowed per switch.	BlackDiamond 12800 R-series	4,076
Hierarchical QoS—maximum number of egress-only traffic queues allowed per switch.	BlackDiamond 12800 R-series	4,076
Hierarchical QoS—maximum number of traffic queues attach per port.	BlackDiamond 12800 R-series	4,076
IGMP sender—maximum number of IGMP senders per switch.	BlackDiamond 8800 c-series BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit series	2,048[c] 1,024 15,000 15,000 1,024
IGMP snooping per VLAN filters—maximum number of VLANs supported in per-VLAN IGMP snooping mode.	Summit X150 Summit X250e Summit X350 Summit X450 Summit X450a Summit X450e BlackDiamond 8800 original BlackDiamond 8800 c-series BlackDiamond 8800 a-series BlackDiamond 8800 e-series	448 448 448 60 1,000 448 60 2,000 1,000 448
IGMPv1/v2 SSM-map entries—maximum number of IGMPv1/v2 SSM mapping entries.	All platforms	500
IGMPv1/v2 SSM-MAP entries—maximum number of sources per group in IGMPv1/v2 SSM Mapping entries.	All platforms	50
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per port.	BlackDiamond 8800 series BlackDiamond 8800 c-series BlackDiamond 10808 BlackDiamond 12800 series Summit series	1,000 2,000 5,000 5,000 1,000
IGMPv2 subscriber—maximum number of IGMPv2 subscribers per switch.	BlackDiamond 8800 series BlackDiamond 8800 c-series BlackDiamond 10808 BlackDiamond 12800 series Summit series	10,000 20,000 30,000 30,000 10,000
IGMPv3 maximum source per group—maximum number of source addresses per group.	All platforms	250

Metric	Product	Limit
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per port.	BlackDiamond 8800 series	1,000
	BlackDiamond 8800 c-series	2,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	Summit series	1,000
IGMPv3 subscriber—maximum number of IGMPv3 subscribers per switch.	BlackDiamond 8800 series	10,000
	BlackDiamond 8800 c-series	20,000
	BlackDiamond 10808	30,000
	BlackDiamond 12800 series	30,000
	Summit series	10,000
IP ARP entries in software—maximum number of IP ARP entries in software.	All platforms	20,480
IPv4 ARP entries in hardware with minimum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with minimum LPM routes present. For BlackDiamond 8800 and Summit series switches, assumes number of IP route reserved entries is 100 or less.	BlackDiamond 8800 c-series	8,000
	BlackDiamond 8800 a-series	8,000
	BlackDiamond 8800 e-series	1,000[d]
	BlackDiamond 8800 original	2,000[d]
	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
	Summit X250e	1,000[d]
	Summit X450	2,000[d]
	Summit X450a	8,000
	Summit X450e	1,000[d]
IPv4 ARP entries in hardware with maximum LPM routes—maximum recommended number of IPv4 ARP entries in hardware, with maximum LPM routes present. For BlackDiamond 8800 and Summit series, assumes number of IP route reserved entries is "maximum."	BlackDiamond 8800 c-series	6,000[d]
	BlackDiamond 8800 a-series	2,000[d]
	BlackDiamond 8800 e-series	500[d]
	BlackDiamond 8800 original	2,000[d]
	BlackDiamond 10808	224,000
	BlackDiamond 12800 series	49,000
	BlackDiamond 12800 R-series	224,000
	Summit X250e	500[d]
	Summit X450	2,000[d]
	Summit X450a	2,000[d]
	Summit X450e	500[d]

Metric	Product	Limit
IPv4 remote hosts in hardware with zero LPM routes—maximum recommended number of IPv4 remote hosts (hosts reachable through a gateway) in hardware when LPM routing is not used. For BlackDiamond 8800 and Summit series, assumes number of IP route reserved entries is 0, and number of IPv4 ARP entries present is 100 or less.	BlackDiamond 8800 c-series	18,000[d]
	BlackDiamond 8800 a-series	14,000[d]
	BlackDiamond 8800 e-series	1,000[d]
	BlackDiamond 8800 original	N/A
	BlackDiamond 10808	N/A
	BlackDiamond 12800 series	N/A
	BlackDiamond 12800 R-series	N/A
	Summit X250e	1,000[d]
	Summit X450	N/A
	Summit X450a	14,000[d]
	Summit X450e	1,000[d]
IPv6 host entries in hardware—maximum number of IPv6 neighbor entries in hardware.	BlackDiamond 8800 c-series	3,000[d]
	BlackDiamond 8800 a-series	1,000[d]
	BlackDiamond 8800 e-series	250[d]
	BlackDiamond 10808	112,000
	BlackDiamond 12800 series	24,500
	BlackDiamond 12800 R-series	112,000
	Summit X250e	250[d]
	Summit X450a	1,000[d]
	Summit X450e	250[d]
IPv4 routes—maximum number of IPv4 routes in software (combination of unicast and multicast routes).	BlackDiamond 8800 series	25,000
	BlackDiamond 10808	1,000,000
	BlackDiamond 12800 series	1,000,000
	Summit series	25,000
IPv4 routes (LPM entries in hardware)— number of IPv4 routes in hardware.	BlackDiamond 8800 c-series	12,000
	BlackDiamond 8800 a-series	12,000
	BlackDiamond 8800 e-series	480
	BlackDiamond 8800 series	8,000
	BlackDiamond 10808	256,000
	MSM-1 MSM-1XL	98,000 229,000
	BlackDiamond 12800 series	
	MSM-5 MSM-5R MSM-6R	49,000 229,000 229,000
	Summit X250e	480
	Summit X450	8,000
	Summit X450a	12,000
	Summit X450e	480

Metric	Product	Limit
IPv6 routes (LPM entries in hardware)—number of IPv6 routes in hardware.	BlackDiamond 8800 c-series BlackDiamond 8800 a-series BlackDiamond 8800 e-series BlackDiamond 10808 BlackDiamond 12800 series Summit X250e Summit X450a Summit X450e	6,000 6,000 240 114,500 114,500 240 6,000 240
IP router interfaces—maximum number of VLANs performing IP routing–excludes sub VLANs (IPv4 and IPv6 interfaces).	All platforms with Edge license or above	512
IP multicast static routes—maximum number of permanent multicast IP routes.	All platforms	1,024
IP unicast static routes—maximum number of permanent IP unicast routes.	All platforms	1,024
IP route sharing (maximum gateways)—configurable maximum number of configurable gateways used by equal cost multipath OSPF, OSPFv3, or static routes.	BlackDiamond 8800 series Summit X250e Summit X450	2, 4, or 8 2, 4, or 8 2, 4, or 8

Metric	Product	Limit
IP route sharing (total destinations)—maximum number of unique destinations used by multipath OSPF, OSPFv3, or static routes.	BlackDiamond 8800 series	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	511 1,023 255
	BlackDiamond 8800 c-series	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	511 1,023 255
	BlackDiamond 8800 a-series	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	511 1,023 255
	BlackDiamond 8800 e-series	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	31 63 15
	BlackDiamond 10808	
	(with up to 8 gateways per destination)	7,136
	BlackDiamond 12800 series	
	(with up to 8 gateways per destination)	7,136
	Summit X250e	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	31 63 15
	Summit X450	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	511 1,023 255
	Summit X450a	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	511 1,023 255
	Summit X450e	
	(default maximum gateways of 4) (if maximum gateways is 2) (if maximum gateways is 8)	31 63 15
IP multinetting (secondary IP addresses)—maximum number of secondary IP addresses per VLAN.	All platforms	64
IS-IS adjacencies—maximum number of supported IS-IS adjacencies.	BlackDiamond 8800 series	128
	Black Diamond 10808	255
	BlackDiamond 12800 series	255
	Summit X450 and X450a	128
IS-IS ECMP—maximum number of equal cost multipath for IS-IS.	BlackDiamond 8800 series (configurable)	2, 4, or 8
	BlackDiamond 10808	8
	BlackDiamond 12800 series	8
	Summit X450 and X450a (configurable)	2, 4, or 8

Metric	Product	Limit
IS-IS interfaces—maximum number of interfaces that can support IS-IS.	All platforms	255
IS-IS routers in an area—recommended maximum number of IS-IS routers in an area.	All platforms	256
IS-IS route origination—recommended maximum number of routes that can be originated by an IS-IS node.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X450 and X450a	20,000 30,000 30,000 5,000
IS-IS IPv4 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8800 series BlackDiamond 10808 MSM-1 MSM-1XL BlackDiamond 12800 series MSM-5 MSM-5R MSM-6R Summit X450 and X450a	25,000 120,000 180,000 100,000 120,000 180,000 5,000
IS-IS IPv4 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8800 series BlackDiamond 10808 MSM-1 MSM-1XL BlackDiamond 12800 series MSM-5 MSM-5R MSM-6R Summit X450 and X450a	25,000 120,000 180,000 100,000 120,000 180,000 5,000
IS-IS IPv4 L1 routes in an L1/L2 router—recommended maximum number of IS-IS Level 1 routes in an L1/L2 IS-IS router.	BlackDiamond 8800 series BlackDiamond 10808 MSM-1 MSM-1XL BlackDiamond 12800 series MSM-5 MSM-5R MSM-6R Summit X450 and X450a	20,000 20,000 25,000 20,000 20,000 25,000 3,000
IS-IS IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router.	BlackDiamond 8800 series BlackDiamond 10808 MSM-1 MSM-1XL BlackDiamond 12800 series MSM-5 MSM-5R MSM-6R Summit X450 and X450a	10,000 30,000 65,000 30,000 40,000 65,000 5,000

Metric	Product	Limit
IS-IS IPv6 L2 routes—recommended maximum number of IS-IS Level 2 routes.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	
	MSM-1	30,000
	MSM-1XL	65,000
	BlackDiamond 12800 series	
	MSM-5	30,000
	MSM-5R	40,000
	MSM-6R	65,000
	Summit X450 and X450a	5,000
IS-IS IPv6 L1 routes in a L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a L1/l2 router.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	
	MSM-1	15,000
	MSM-1XL	25,000
	BlackDiamond 12800 series	
	MSM-5	15,000
	MSM-5R	15,000
	MSM-6R	25,000
	Summit X450 and X450a	3,000
IS-IS IPv4/IPv6 L1 routes in an L1 router—recommended maximum number of IS-IS Level 1 routes in a Level 1 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8800 series	20,000
	BlackDiamond 10808	
	MSM-1	60,000
	MSM-1XL	130,000
	BlackDiamond 12800 series	
	MSM-5	30,000
	MSM-5R	60,000
	MSM-6R	130,000
	Summit X450 and X450a	5,000
IS-IS IPv4/IPv6 L2 routes in an L2 router—recommended maximum number of IS-IS Level 2 routes in a Level 2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8800 series	20,000
	BlackDiamond 10808	
	MSM-1	60,000
	MSM-1XL	130,000
	BlackDiamond 12800 series	
	MSM-5	30,000
	MSM-5R	60,000
	MSM-6R	130,000
	Summit X450 and X450a	5,000
IS-IS IPv4/IPv6 L1 routes in a L1/L2 router—recommended maximum number of IS-IS Level 1 routes in a Level 1/Level2 IS-IS router. The numbers documented are based on 50% IPv4 routes and 50% IPv6 routes.	BlackDiamond 8800 series	20,000
	BlackDiamond 10808	20,000
	BlackDiamond 12800 series	20,000
	Summit X450 and X450a	3,000
Jumbo frames—maximum size supported for jumbo frames, including the CRC.	All platforms	9,216

Metric	Product	Limit
Load sharing groups—maximum number of load share groups. **Note:** The actual number of load share groups that can be configured is limited by the number of physical ports present in the switch or SummitStack.	BlackDiamond 8800 series	
	with 10G4X	32
	without 10G4X	128
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	Summit X150 and X350 series	32
	Summit X250e	32
	Summit X450	32
	SummitStack	
	with Summit X450-24t	32
	with Summit X450-24x	32
	without Summit X450-24t	128
	without Summit X450-24x	128
Load sharing—maximum number of ports per load share group.	BlackDiamond 8800 series	8
	BlackDiamond 10808	16
	BlackDiamond 12800 series	16
	Summit series	8
Logged messages—maximum number of messages logged locally on the system.	All platforms	20,000
MAC-based security—maximum number of MAC-based security policies.	All platforms	1,024
MAC-in-MAC—maximum number of MAC FDB entries (MAC addresses on the local side) and MAC binding entries (MAC addresses on remote side).	BlackDiamond 10808	100,000
	BlackDiamond 12800 series	100,000
MAC-in-MAC—maximum number of regular VLANs (VLAN, vMAN, BVLAN).	BlackDiamond 10808	4,000
	BlackDiamond 12800 series	4,000
MAC-in-MAC—maximum number of SVLANs.	BlackDiamond 10808 (1G DRAM)	2,000
	BlackDiamond 12800 series (512 DRAM)	2,000
Mirroring (filters)—maximum number of mirroring filters.	All platforms	16
Mirroring (monitor port)—maximum number of monitor ports.	All platforms	1
Mirroring, one-to-many (filters)—maximum number of one-to-many mirroring filters.	All platforms	16
Mirroring, one-to-many (monitor port)—maximum number of one-to-many monitor ports.	All platforms	16
MPLS LDP enabled interfaces—maximum number of MPLS LDP configured interfaces per switch.	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
MPLS LDP peers—maximum number of MPLS LDP peers per switch.	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
MPLS LDP adjacencies—maximum number of MPLS LDP adjacencies per switch.	BlackDiamond 10808	50
	BlackDiamond 12800 R-series	50

Metric	Product	Limit
MPLS LDP labels—maximum number of MPLS LDP labels per switch.	BlackDiamond 10808* BlackDiamond 12800 R-series* *It may take a long time to converge and populate the labels in hardware.	20,000 18,000
MPLS static LSPs—maximum number of static LSPs.	BlackDiamond 10808 BlackDiamond 12800 R-series	1,000 1,000
MSDP active peers—maximum number of active MSDP peers.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X450	32 32 32 16
MSDP SA cache entries—maximum number of entries in SA cache.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X450	16,000 16,000 16,000 8,000
MSDP maximum mesh groups—maximum number of MSDP mesh groups.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X450	8 8 8 4
Multicast VLAN registration (MVR)—maximum number of senders per switch.	BlackDiamond 8800 series BlackDiamond 8800 c-series BlackDiamond 10808 BlackDiamond 12800 series Summit series	1,024 2,048 15,000 15,000 1,024
Network Login—maximum number of clients being authenticated on MAC-based VLAN enabled ports.	BlackDiamond 8800 series (clients per module/per system) BlackDiamond 12804 (per system) Summit X250e (per system) Summit X450 (per system)	1,024 4,000 1,024 1,024
Network Login—maximum number of dynamic VLANs.	All platforms	2,000
OSPF adjacencies—maximum number of supported OSPF adjacencies.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X250e Summit X450	128 255 255 128 128
OSPF areas—as an ABR, how many OSPF areas are supported within the same switch.	All platforms	8
OSPF ECMP—maximum number of equal cost multipath OSPF.	BlackDiamond 8800 series (configurable) BlackDiamond 10808 BlackDiamond 12800 series Summit X250e (configurable) Summit X450 (configurable)	2, 4, or 8 8 8 2, 4, or 8 2, 4, or 8

Metric	Product	Limit
OSPF external routes—recommended maximum number of external routes contained in an OSPF LSDB without too many other types of OSPF routes.	BlackDiamond 8800 series	20,000
	BlackDiamond 10808	130,000
	BlackDiamond 12800 series	130,000
	Summit X250e	5,000
	Summit X450	5,000
OSPF inter- or intra-area routes—recommended maximum number of inter- or intra-area routes contained in an OSPF LSDB without too many other types of OSPF routes, with one ABR in OSPF domain.	BlackDiamond 8800 series	7,000
	BlackDiamond 10808	7,000
	BlackDiamond 12800 series	7,000
	Summit X250e	2,000
	Summit X450	2,000
OSPF routers in a single area—recommended maximum number of routers in a single OSPF area.	BlackDiamond 8800 series	100
	BlackDiamond 10808	200
	BlackDiamond 12800 series	100
	Summit X250e	50
	Summit X450	50
OSPF subnets on a single router—recommended maximum number of OSPF routed subnets on a switch.	All platforms with Core license or above	400
OSPF virtual links—maximum number of supported OSPF virtual links.	All platforms with Core license or above	32
OSPFv3 areas—as an ABR, the maximum number of supported OSPFv3 areas.	All platforms with Core license or above	16
OSPFv3 interfaces—maximum number of OSPFv3 interfaces.	BlackDiamond 8800 series	256
	BlackDiamond 10808	384
	BlackDiamond 12800 series	256
	Summit X450	128
	Summit X450a	128
OSPFv3 neighbors—maximum number of OSPFv3 neighbors.	BlackDiamond 8800 series	64
	BlackDiamond 10808	128
	BlackDiamond 12800 series	128
	Summit X450	64
	Summit X450a	64
OSPFv3 virtual links—maximum number of OSPFv3 virtual links supported.	All platforms with Core license or above	16
OSPFv3 external routes—recommended maximum number of external routes.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	60,000
	BlackDiamond 12800 series	50,000
	Summit X450	10,000
	Summit X450a	10,000

Metric	Product	Limit
OSPFv3 inter- or intra-area routes—recommended maximum number of inter- or intra-area routes.	BlackDiamond 8800 series	6,000
	BlackDiamond 10808	6,000
	BlackDiamond 12800 series	6,000
	Summit X450	3,000
	Summit X450a	3,000
PIM snooping—maximum number of (S,G) entries programmed in the hardware.	BlackDiamond 8800 series	1,024
	BlackDiamond 8800 c-series	2,048
	BlackDiamond 10808	12,000
	BlackDiamond 12800 series	12,000
	Summit series	1,024
PIM—maximum routes—maximum number of (S,G) entries installed in the hardware.	BlackDiamond 8800 series	1,024
	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 10808	12,000
	BlackDiamond 12800 series	12,000
	Summit series	1,024
PIM-SSM (maximum SSM routes)—maximum number of (S,G) entries installed in the HW with PIM SSM configuration.	BlackDiamond 8800 series	1,024
	BlackDiamond 8800 c-series	2,048[c]
	BlackDiamond 10808	15,000
	BlackDiamond 12800 series	15,000
	Summit series	1,024
PIM (maximum interfaces)—maximum number of PIM active interfaces.	All platforms	256
PIM (maximum interfaces)—maximum number of PIM snooping enabled interfaces.	All platforms	256
Policy-based routing (PBR) redundancy—maximum number of flow-redirect and nexthops per each flow-direct.	All platforms	32
Private VLANs—maximum number of subscribers. Assumes a minimum of one port per network and subscriber VLAN.	BlackDiamond 8800 a-, c-, and e-series	
	with eight modules of 48 ports	383
	BlackDiamond 10808	1,400
	BlackDiamond 12800 series	1,400
	Summit X450a and X450e, 24 port	
	with two-port option card	25
	without option card	23
	Summit X450a and X450e, 48 port	
	with two-port option card	49
	without option card	47
Private VLANs—maximum number of private VLANs with an IP address on the network VLAN.	All platforms	512
Private VLANs—maximum number of private VLANs in an L2-only environment.	All platforms	2,046

Metric	Product	Limit
Provider Backbone Bridging-Traffic Engineering (PBB-TE)—maximum number of static MAC binding entries.	BlackDiamond 10808	
	MSM-1	98,000
	MSM-1XL	100,000
	BlackDiamond 12800 series	
	MSM-5	49,000
	MSM-5R	100,000
	MSM-6R	100,000
Route policies—suggested maximum number of lines in a route policy file.	All platforms	10,000
RIP-learned routes—maximum number of RIP routes supported without aggregation.	BlackDiamond 8800 series	10,000
	BlackDiamond 10808	10,000
	Summit X250e	3,000
	Summit X450	3,000
RIP interfaces on a single router—recommended maximum number of RIP routed interfaces on a switch.	BlackDiamond 8800 series	256
	BlackDiamond 10808	384
	Summit X250e	128
	Summit X450	128
RIPng learned routes—maximum number of RIPng routes.	BlackDiamond 8800 series	3,000
	BlackDiamond 10808	5,000
	BlackDiamond 12800 series	5,000
	Summit X250e	1,500
	Summit X450	1,500
RSVP-TE interfaces—maximum number of interfaces.	BlackDiamond 10808	32
	BlackDiamond 12800 R-series	32
RSVP-TE neighbors—maximum number of neighbors per interface.	BlackDiamond 10808	400
	BlackDiamond 12800 R-series	400
RSVP-TE ingress LSPs—maximum number of ingress LSPs.	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	2,000
RSVP-TE egress LSPs—maximum number of egress LSPs.	BlackDiamond 10808	4,000
	BlackDiamond 12800 R-series	3,000
RSVP-TE transit LSPs—maximum number of transit LSPs.	BlackDiamond 10808	2,000
	BlackDiamond 12800 R-series	1,500
RSVP-TE paths—maximum number of paths.	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
RSVP-TE profiles—maximum number of profiles.	BlackDiamond 10808	1,000
	BlackDiamond 12800 R-series	1,000
RSVP-TE EROs—maximum number of EROs per path.	BlackDiamond 10808	64
	BlackDiamond 12800 R-series	64
Spanning Tree (maximum STPDs)—maximum number of Spanning Tree Domains on port mode EMISTP.	All platforms	64
Spanning Tree PVST—maximum number of port mode PVST domains.	All platforms	128

Metric	Product	Limit
Spanning Tree—maximum number of multiple spanning tree instances (MSTI) domains.	All platforms	64
Spanning Tree—maximum number of VLANs per MSTI.	All platforms	500
Spanning Tree—maximum number of VLANs on all MSTP instances.	All platforms	1,000
Spanning Tree (802.1d domains)—maximum number of 802.1d domains per port.	All platforms	1
Spanning Tree (number of ports)—maximum number of ports including all Spanning Tree domains.	All platforms	2,048
Spanning Tree (maximum VLANs)—maximum number of STP protected VLANs.	dot1d dot1w	560 560
SSH (number of sessions)—maximum number of simultaneous SSH sessions.	All platforms	8
Static MAC multicast FDB entries—maximum number of permanent multicast MAC entries configured into the FDB.	BlackDiamond 8800 original series BlackDiamond 8800 c-series BlackDiamond 8800 a-series BlackDiamond 8800 e-series BlackDiamond 10808 BlackDiamond 12800 series Summit X150 and X350 series Summit X250e Summit X450 original series Summit X450e Summit X450a	256 1,024 1,024 1,024 1,024 1,024 1,024 1,024 256 1,024 1,024
Syslog servers—maximum number of simultaneous syslog servers that are supported.	All platforms	4
TCAM entries—amount of entries available in the lookup tables for Longest Prefix Match routing lookups, learned MAC address, and ACLs.	BlackDiamond 10808, MSM-1 BlackDiamond 10808, MSM-1XL BlackDiamond 12800 series BlackDiamond 12800 R-series	128,000 256,000 49,000 229,000
Telnet (number of sessions)—maximum number of simultaneous Telnet sessions.	All platforms	8
Virtual routers—number of user virtual routers that can be created on a switch.	BlackDiamond 8800 series BlackDiamond 10808 BlackDiamond 12800 series Summit X250e Summit X450	Not supported 8 8 Not supported Not supported
VLAN aggregation—maximum number of port-VLAN combinations on any one super VLAN and all of its sub VLANs.	All platforms	1,000
VLANs—includes all VLANs.	All platforms	4,094
VLANs—maximum number of ports.	BlackDiamond 12804	50,029
VLANs (Layer 2)—maximum number of Layer 2 VLANs.	All platforms	4,094

Metric	Product	Limit
VLANs (Layer 3)—maximum number of Layer 3 VLANs.	All platforms	512
VLANs (maximum active port-based)—number of simultaneously active port-based VLANs.	All platforms	4,094
VLANs (maximum active protocol-sensitive filters)—number of simultaneously active protocol filters in the switch.	All platforms	15
VLAN translation—maximum number of translation VLANs. Assumes a minimum of one port per translation and member VLAN.	BlackDiamond 8800 a-, c-, and e-series with eight modules of 48 ports BlackDiamond 10808 BlackDiamond 12800 series Summit X450a and X450e, 24 port with two-port option card without option card Summit X450a and X450e, 48 port with two-port option card without option card	 383 1,400 1,400 25 23 49 47
VLAN translation—maximum number of translation VLAN pairs with an IP address on the translation VLAN.	All platforms	512
VLAN translation—maximum number of translation VLAN pairs in an L2 only environment.	All platforms	2,046
vMAN (maximum ACL rules for vMAN)—maximum number of ACL rules for vMAN.	BlackDiamond 10808 BlackDiamond 12800 series	4,000 4,000
VPLS: VCCV (pseudo wire Virtual Circuit Connectivity Verification) VPNs—maximum number of VCCV enabled VPLS VPNs.	BlackDiamond 10808 BlackDiamond 12800 R-series	16 16
VPLS: MAC addresses in an H-VPLS network—maximum number of MAC address learned by a switch in an evenly distributed hierarchical VPLS **Note:** Increasing the number of spokes per VPLS will decrease the maximum number of MAC addresses that can be learned.	BlackDiamond 10808 BlackDiamond 12800 R-series	60,000 60,000
VPLS: MAC addresses in a fully meshed VPLS network—maximum number of MAC addresses learned by a switch in an evenly distributed fully meshed VPLS network.	BlackDiamond 10808 BlackDiamond 12800 R-series	100,000 80,000
VPLS VPNs—maximum number of VPLS virtual private networks per switch.	BlackDiamond 10808 BlackDiamond 12800 R-series	500 point-to-point 500 point-to-point
VPLS peers—maximum number of VPLS peers per switch.	BlackDiamond 10808 BlackDiamond 12800 R-series	16 16
VPLS pseudo wires—maximum number of VPLS pseudo wires per switch.	BlackDiamond 10808 BlackDiamond 12800 R-series	1,000 500
VRRP (maximum instances)—maximum number of VRRP supported VLANs for a single switch.	All platforms with Advanced Edge license or above	128

Metric	Product	Limit
VRRP (maximum VRID)—maximum number of unique VRID numbers per switch.	All platforms with Advanced Edge license or above	7
VRRP (maximum VRIDs per VLAN)—maximum number of VRIDs per VLAN.	All platforms with Advanced Edge license or above	7
VRRP (maximum ping tracks)—maximum number of ping tracks per VLAN.	All platforms with Advanced Edge license or above	8
VRRP (maximum ping tracks)—maximum number of ping tracks per VRRP Instance under 128 VRRP instances. Hello interval: 100 milliseconds Frequency: 3 seconds Miss: 3 Hello interval: 1 second Frequency: 3 seconds Miss: 3	All platforms with Advanced Edge license or above	 2 4
VRRP (maximum iproute tracks)—maximum number of iproute tracks per VLAN.	All platforms with Advanced Edge license or above	8
VRRP—maximum number of VLAN tracks per VLAN.	All platforms with Advanced Edge license or above	8
XML requests—maximum number of XML requests per second. **Note**: Limits are dependent on load and type of XML request. These values are dynamic ACL data requests.	BlackDiamond 8800 c-series with 100 DACLs with 100 DACLs with 500 DACLs BlackDiamond 12800 series with MSM-6R with 100 DACLs with 500 DACLs Summit X450a with 100 DACLs with 500 DACLs	 10 3 10 3 4 1

a. An ACL mask defines a unique match criteria and relative rule precedence. Masks are automatically generated based on the contents of an access-list policy. Only adjacent rules within the policy that have identical match criteria will utilize the same ACL mask. For this reason, it is advantageous to list all rules with the same match criteria together unless a relative precedence with other policy rules is required. Using VLAN-based or wildcard ACLs requires the ACL masks to be allocated on every port in the system.
b. The table shows the total available; see the note included in PD3-77983510.
c. Applies only if all enabled BlackDiamond I/O modules are BlackDiamond 8800 c-series modules.
d. Effective capacity varies based on actual IP addresses and hash algorithm selected, but is higher for BlackDiamond 8800 c-series modules compared to BlackDiamond 8800 a-series and e-series modules.

4 Open Issues, Known Behaviors, and Resolved Issues

This chapter describes items needing further clarification, known behaviors that might not be intuitive, and resolved issues.. The numbers shown in column one of the following tables are for internal reference and can be ignored.

This chapter contains the following section:

- Open Issues on page 134
- Known Behaviors on page 148
- Resolved Issues in ExtremeXOS 12.1.4-patch1-9 on page 153
- Resolved Issues in ExtremeXOS 12.1.4-patch1-8 on page 153
- Resolved Issues in ExtremeXOS 12.1.4-patch1-7 on page 154
- Resolved Issues in ExtremeXOS 12.1.4-patch1-6 on page 154
- Resolved Issues in ExtremeXOS 12.1.4-patch1-5 on page 155
- Resolved Issues in ExtremeXOS 12.1.4-patch1-4 on page 155
- Resolved Issues in ExtremeXOS 12.1.4-patch1-3 on page 156
- Resolved Issues in ExtremeXOS 12.1.4-patch1-2 on page 156
- Resolved Issues in ExtremeXOS 12.1.4-patch1-1 on page 157
- Resolved Issues in ExtremeXOS 12.1.4 on page 158
- Resolved Issues in ExtremeXOS 12.1.3-patch1-9 on page 159
- Resolved Issues in ExtremeXOS 12.1.3-patch1-8 on page 160
- Resolved Issues in ExtremeXOS 12.1.3-patch1-6 on page 161
- Resolved Issues in ExtremeXOS 12.1.3-patch1-4 on page 163
- Resolved Issues in ExtremeXOS 12.1.3-patch1-2 on page 165
- Resolved Issues in ExtremeXOS 12.1.3 on page 167
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-17 on page 170
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-15 on page 171
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-12 on page 172
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-10 on page 173
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-7 on page 174
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-4 on page 174
- Resolved Issues in ExtremeXOS 12.1.2.17-patch1-3 on page 176
- Resolved Issues in ExtremeXOS 12.1.2.17 on page 177
- Resolved Issues in ExtremeXOS 12.1.1.4 on page 180
- Resolved Issues in ExtremeXOS 12.1.0.29 on page 183

Open Issues

Following are the open issues for supported features in ExtremeXOS 12.1. They are organized into the following sections:

Table 32: Platform-Specific and Feature PDs

PD Number	Description
General	
PD3-210656503, PD4-331224298	**Log Filter With a Target Session Cannot be Deleted** A log filter configured with a target session cannot be deleted after logging out of a switch and then logging back in.
PD4-254500398	**Each IP Address Configured VLAN Occupies Two LPM Hardware Entries Instead of One** Each IP address configured VLAN occupies two longest prefix match (LPM) hardware entries instead of one. One entry is for the directly attached subnet, and the other is a host route for the interface itself. This issue affects the recommended value for the `configure iproute reserved-entries` command. See the *ExtremeXOS 12.1.2 Command Reference Guide* for new usage guidelines.
PD3-190363671	**Hot Swapping PSUs Generates an Error Message** The following error message is displayed while hot swapping PSUs: `Unable to read PSU-2 FRU data. Try reinserting PSU more quickly.` **Workaround:** Remove and reinsert the PSU quickly. Insert the PSU in a single, continuous motion with a firm push.
PD3-207678214	**User-Configured Banner Remains Active** The user-configured banner remains active when rebooting a switch without first saving the configuration.
PD3-207576821	**Upgrading the BootROM to the Minimum Version on an MSM-6R is Not Working Correctly** Upgrading the BootROM 1.0.1.8 on an MSM-6R running ExtremeXOS 12.0.2.25 software is not working correctly. If you run the `install firmware` command and then reboot the switch, the BootROM version remains 1.0.1.8.
PD3-206179541	**Most L3 Traffic Slow Path Forwarded if IP Route Compression is Enabled** Enabling IP route compression on a BlackDiamond 10808 or 12800 series switch that has already reached the maximum IPv4 routing entries in hardware might cause slow path forwarding for some of the L3 traffic.
PD3-202580681	**Some L3 Traffic May Temporarily Be Slow Path Forwarded When IP Route Compression is Enabled** Enabling IP route compression may cause temporary slow path forwarding for some of the L3 traffic.
PD3-192821161	**Maximum Number of Supported IPv4 and IPv6 Interfaces** For Summit X450 a-series and e-series switches, and the BlackDiamond 8800 series of switches, the maximum number of supported IP interfaces is 512 (IPv4 and IPv6 combined). If there are more IP interfaces configured, the following log message is displayed: `12/11/2007 06:06:14.73 <Info:HAL.VLAN.Info> Maximum # of IP interfaces (512) already configured. Could not add IP address 0x0A010101 mask 0xFFFFFF00`

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-201570011	**Relay Agent IP Address Should be Configured as the Trusted Server** When dhcp-relay is configured in a DHCP snooping environment, the relay agent IP address should be configured as the trusted server. If the relay agent IP address is not configured as the trusted server, DHCP responses are blocked.
PD3-190574171	**Ports May Stay in Active State Even After the Cable is Disconnected** Ports on Summit X450a and X450e series switches may stay in an active state even after the cable is disconnected with certain QoS configurations.
PD3-132775269	**Telnet Sessions Between Two Switches Causing Mount/Remount Problem** Telnet sessions between two switches using two windows causes one session to hang if both sessions are edited and but only one session is saved.
BlackDiamond 8800 Series Switch	
PD4-1014993561, PD4-690502742	**Inserting I/O Module in Slot B Generates an Error** The following error is displayed when inserting an I/O module into slot B in a supported environment. `<Erro:Kern.Erro r> MSM-A: ahd: Error reading io expander for slot 12 rc=-1` This message is seen only when an I/O module is in use in slot B. It is logged when an I/O module is inserted in slot B, or when the chassis boots with an I/O module in slot B. Having an I/O module in slot B is supported while using any MSM other than MSM-128. This log message can be ignored as there is no impact to system functionality or performance.
BlackDiamond 10808 Switch	

PD3-124124316	**Unicast Routes with ECMP Enabled Causes Log Errors**
	The following error messages are shown in the log when running 50,000 unicast routes with ECMP enabled:
	`02/05/2007 15:38:37.89 <Warn:HAL.Sys.Warning> MSM-A: hal: Reached maximum otp index allocation`
	`02/05/2007 15:38:37.56 <Warn:HAL.Sys.Warning> MSM-A: Previous message repeated 999 additional times in the last 1 second(s)`

PD3-68165111	**System Health Check Parity Walk Verification Function Should be Enabled** Various memory locations that are part of the forwarding and routing tables are parity protected on BlackDiamond 10808 switches. The functionality should be turned on so that faults are detectable.

PD3-41204902	**Output for the "show platform ipv4mc group <group address>" Command Contains an “invalid” Entry**
	The output for the `show platform ipv4Mc group <group address>` command contains an “invalid” entry.
	`BD-10808.61 # show platform ipv4Mc g 239.255.255.1`
	`Total Entries:27`
	`Index Type VrId Port Source Group PTI Vlan`
	`004A6 -> 03E3A [3] - invalid`

PD3-14127903, PD3-13538171	**Egress Mirror Packets are Being Sent to Mirror Port in Link Down State** Mirrored egress packets are being sent to the mirror port even when the port is in the link down state.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
BlackDiamond 12800 Series Switches	
PD3-187808062	**Switch Does Not Show Warning Message for Down Revision MSM and I/O Modules** A BlackDiamond 12800 series switch does not show a warning message on the console for down revision MSM and I/O modules after initialization.
PD3-24601141	**802.1P Precedence Support** Incoming 802.1P precedence is not supported when ports are used for vMAN.
PD3-125511903	**System Fails with a Signal 10 Error When Running an MSM Failover** A system failure occurs with a signal 10 error when performing a run msm-failover immediately after the backup MSM is in-sync
PD3-130441271, PD4-281640171	**Traffic Queues with Metering are Not Applied Correctly** Traffic queues with metering are not applied correctly with large packets, such as 256, 512, and 1,024. The traffic fluctuates between different rates when the packet size is above 200.
PD3-86738591	**Traffic Queue Statistics are Incorrect when Switch is Configured** Traffic queue statistics are incorrect when a BlackDiamond 12800 series switch is configured to work in H-QoS mode. Statistics counters are accurate when the switch is configured in the PRI mode.
PD3-98333969	**Disabling and Enabling a Port Can Take 30 Seconds for Port to Activate** During continuous FDB learning, disabling/enabling a port can take up to 30 seconds for the port to activate.
Summit Family of Switches	
PD4-310814981	**When Configuring a Set of ACLs, Performing a Save and a Reboot Generates an Error** When configuring a set of ACLs on a Summit X450a-48t switch, the access control lists are successfully applied, however, performing a save and a reboot generates an error.
PD3-204517991	**Summit X250e-24x Combo Port Link May Come Up With the Correct Speed But in Half-Duplex Mode** A Summit X250e-24x combo port link may come up with the correct speed but in half-duplex mode, even though the switch is configured as full-duplex mode when autonegotiation is set to off on both sides of the link. For the link to come up in full-duplex mode as configured, you must disable and enable the port, or restart the port.
PD3-201233169	**Port Does Not Come up After Disable/Enable or Reboot on Some Mitel IP Phones** A condition exists with some Mitel IP phones that are attached to an ExtremeXOS PoE enabled platform that requires that you disable and enable inline power in order for the phone to become active.
PD3-131375426	**Autopolarity Does Not Work on Combo Ports** Configuring autopolarity does not work on the combo ports on the Summit family of switches.
PD3-77711011	**“Slot” Should Not be Included in “show inline-power stats” Command Output** The word “slot” should not be included in the output of the `show inline-power stats` command.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-77711042	**Priority Column Should Not be Included in "show inline-power configuration" Command Output** The Priority column should not display in the output of the `show inline-power configuration` CLI command when running the command on a Summit X450-24p PoE switch.

PD3-43606168	**"show log" Command Output Filled with sFlow Receiver Missing Message**
	If sFlow does not have a collector configured using the `configure sflow collector` command, the `show log` command generates the following messages:
	`08/23/2005 12:28:09.55 <Noti:sflow.debug.AddCntSmplFail> : Could not add the counter sample for port 0:1020, as receiver is not configured.`
	`08/23/2005 12:07:49.55 <Noti:sflow.debug.AddCntSmplFail> : Previous message repeated 61 additional times in the last 1200 second(s).`

PD3-40266236, PD3-40233121	**Redundant Ports Not Correctly Moving to Other Ports in Load Sharing Mode** Traffic on load share ports configured as redundant ports incorrectly moves to other ports in the load share group during link transition.
SummitStack	
PD3-209191744	**Link State May Not be Correct on a Redundant Port** After running the `disable port all` command on a switch that is configured with a redundant port, the link state may not always be correct.
PD3-209191768	**Some Port LEDs May Light Green Even Though Ports are Not Up** After running the `disable port all` command on a SummitStack, some port LEDs may sometimes light green even though ports are not up.
PD3-204744742	**Ping in VR-Mgmt in SummitStack Displays Node Address Instead of MAC Address** IPv6 neighbor-discovery in a management VLAN in a SummitStack resolves to the node address of the stack master, instead of the stack MAC address.
ACL	
PD3-192175421	**Installing a Policy File May Generate an Error Message** The following error message is displayed when installing a policy file with more than 4,096 rules: `Error: Unable to bind traffic queue tq4095 to port 1:1.`
PD3-127190211	**VLAN ACLs Do Not Work When vMAN Ethertype is Set to 0x8100** Using a BlackDiamond 10808 or a 12800 series switch, VLAN ACLs do not work when a vMAN EtherType is set to 0x8100. Incoming traffic is not matched against the rules in the ACL policy file and the traffic is forwarded without applying the matched rule in the policy file.
PD3-118223441, PD3-57946832, PD3-26612201, PD3-24794592	**Before Changing a VLAN Tag, Unconfigure all ACLs Applied to the VLAN** Before changing a VLAN tag, make sure you unconfigure all the ACLs applied to the VLAN. Also, after changing the tag, reconfigure the ACLs to be applied on the VLAN.This applies to BlackDiamond 10808 and 12800 series switches only.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-127842058, PD3-127842159	**Only Ingress Applied CLEAR-Flow Rules are Triggered** With CLEAR-Flow enabled, only ingress applied CLEAR-Flow rules are triggered.
PD3-126824622	**IPv6 Protocol ICMP Should Not be Allowed** If an IPv6 address is included in a configuration, use ICMPv6 for the protocol. ICMP (IPv4) should not be allowed.
PD3-77983510	**Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series Modules: Boot Time and Timing for Applying ACLs** Summit X450a and Summit X450e series switches and BlackDiamond 8800 a-series and e-series modules provide more powerful ACL capabilities. Because of this, the amount and complexity of ACL rules will naturally impact the time needed to process and apply the ACL rules to the switch. This will also impact switch bootup time. Access Control List limitations fall into two areas: physical and virtual. Physical Limits—Summit X450a and Summit X450e series switches: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the Summit X450e and 2048 rules for the Summit X450a. Physical Limits—BlackDiamond 8800 a-series and e-series modules: The per-VLAN, wildcard (port any), and single-port access list installation limitations are 1024 rules for the e-series modules, and 2048 rules for the a-series modules. Extreme Networks recommends that you configure ACLs as per-VLAN, wildcard, or single-port. If either of the following is true, you will have to configure ACLs with multi-port lists: Your application requires that ports do not have a homogeneous ACL policy. When BlackDiamond 8800 original series modules are operational in the same chassis, it may be necessary to configure ACLs to specific port-lists instead of as wildcard or per-VLAN. This is because the original series modules have smaller physical limits. Virtual Limits—Summit X450a and Summit X450e series switches: When configuring a multi-port ACL, use the following guideline. The total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list is supported (1,000 rules * 48 ports in the list <= 48,000). Virtual Limits—BlackDiamond 8800 a-series and e-series modules: When configuring a multi-port ACL, use the following guideline. For any a-series or e-series blade in the system, its total ACL count (as calculated by ACL rules times ports applied to) should not exceed 48,000 total ACL rules. For example, applying a 1,000 rule policy file to a 48 port multi-port list on an a-series module on slot 1 and an e-series module in slot 2 is fine. Neither module exceeds the 48,000 total ACL rules. Excessive boot times and CPU resource starvation can be seen with larger total rule counts. If your application requires additional capacity, contact Extreme Networks.
PD3-28320363	**Invalid Encapsulate Value for IPv6** In IPv6, the encapsulate value is “next header,” which is not currently a valid attribute.
BGP	
PD3-209442785	**Static Multicast Route Will Not be Exported Using MBGP.** Static multicast routes are not exported using MBGP. However, a static unicast route can be exported using MBGP.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
CLEAR-Flow	
PD4-278443631	**CLEAR-Flow Commands Display on Platforms That Do Not Support This Capability** CLEAR-Flow commands display on platforms that do not support this capability, including the Summit X150, X250, X350, and X450e series switches, as well as BlackDiamond 8800 non-c-series switches.
CLI	
PD3-71725881	**Timezone/DST Name Truncates at Seven Characters** When configuring an optional name for the timezone/DST on the Summit X450 family of switches, the timezone name truncates at seven characters. The system default is six characters.
PD3-57182431	**RX Align Counter is Not Incremented** For the incoming traffic with alignment errors, the "RX Align" counter in the output of the `show ports <port number> rxerrors` command is not incremented. Instead the "RX CRC" counter is incremented.
PD3-63858286	**"upload configuration" Command Contains RIP Configuration Commands** The `upload configuration` CLI command contains RIP configuration commands in spite of there not being a RIP VLAN.
Control Protocols	
PD3-125288233	**MSTP Fails to Converge when Ethernet Type is 0x8100** MSTP fails to converge when a vMAN Ethernet type is set to 0x8100 on a BlackDiamond 12800 series switch.
Device Management	
PD3-126243853	**HTTPS with Key Length of 4,096 has High CPU Utilization** Using a key length of 4,096 in an SSL certificate causes high CPU utilization during HTTPS sessions.
Diagnostics	
PD4-285686375	**EEPROM Error Message Appears in Log After Upgrade** After upgrading to the latest ExtremeXOS 12.1.2.17 image, the following EEPROM error message appears in the log: `07/03/2008 12:30:03.72 MSM-A: MSM-B card eeprom checksum failed. 0xb97 != 0xb96`
PD3-204419978	**Repeatedly Running Diagnostics on MSM-48 or MSM-G8x Modules May Fail** Repeatedly running diagnostics on an MSM-48 or an MSM-G8x module may sometimes fail, resulting in the error `EEPROM memory test failed`.

PD3-203116541	**MSM A and MSM B May Display EEPROM Checksum Failed Error**
	Following EEPROM checksum failed error messages may be seen in the syslog:
	`MSM-B card eeprom checksum failed. 0xb8a != 0xb89`
	`MSM-A card eeprom checksum failed. 0xb66 != 0xb65`
	`Backplane eeprom checksum failed. 0xd71 != 0xcd5`

EAPS	
PD4-326832374	**Streams Are Flooded in All Active Ports for the Temporary Flood Duration** Streams are flooded in all active ports for the temporary flood duration after running the `restart ports all` command because a kill entry is not getting installed.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD4-314278544	**Traffic Drop Occurs When Changing an EAPS State** A traffic drop is seen when an EAPS state changes from link-down to link-up even with add-link ports on.
PD3-104885349	**Traffic Loss Occurs When a Shared Link Comes Up** When traffic is running between shared links, FDB entries are incorrectly learned on BlackDiamond 10808 and BlackDiamond 12804 switches. Traffic loss occurs until the incorrectly learned FDB entries age out.
PD3-97153785	**If Multiple Shared Links are Down, a Loop is Created** In a specific EAPS topology, if multiple shared links are down, a loop is created.
PD3-54870537, PD3-45729158	**EAPS with Load Sharing Enabled/Disabled Causes Control Packets to be Received on Port** Misconfigured EAPS control VLAN ports may not be detected, causing EAPS PDUs to be accepted into the system even though they were received on an incorrect port.
ESRP	
PD3-52741820	**Disabling a Shared Port Makes the ESRP Port Restart Configuration Disappears** Disabling a shared port results in the ESRP port restarting and the configuration disappearing.
IP Routing Protocols	
PD3-132508261	**MTU Size for a VLAN is Not Configured** When issuing the `enable jumbo-frame port all` command on a BlackDiamond 8800, the MTU size for the VLAN is not configured. Sending 5,000 byte traffic works correctly. However, if you disable jumbo-frames on the egress port the error message `Packet too big` is displayed.
IPv6 Unicast	

PD3-139714881	**Info Level Messages in Log When Configuring Link Aggregation on VLAN Associated with IPv6 Tunnel**
	The following info level messages appear in the log when link aggregation is configured on a VLAN associated with an IPv6 6-to-4 tunnel:
	`05:01:49.04 <Info:HAL.VLAN.Info> MSM-B: pibIPv6InstallTunneledLinkLocalFilter: Could not install filter unit 12, Entry exists`
	`04/24/2007 05:01:49.05 <Info:HAL.VLAN.Info> MSM-B: pibIPv6InstallTunneledLinkLocalFilter: Repaired filter unit 12`
	These messages do not affect the operation of the switch.

IS-IS	
PD3-206929752	**IS-IS Graceful Restart Fails With Cisco Neighbor** The ExtremeXOS implementation of IS-IS supports draft-ietf-isis-restart-02. As a result, IS-IS graceful restart vendor interoperability is limited to devices which support draft-ietf-isis-restart-03 or earlier.
PD3-190952336	**Graceful Restart for IS-IS May Fail for the Entire Node** When one or more point-to-point interfaces are present on a router with IS-IS graceful restart enabled, the graceful restart may fail for the entire node. **Workaround:** Do not use point-to-point links if graceful restart is also used.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-183234835	**Graceful Restart Fails During "restart process isis"** When one or more point-to-point interfaces are present on a router with graceful restart enabled, the graceful restart may fail for the entire node. **Workaround:** Do not use point-to-point links if graceful restart is also used.
Mirroring	
PD3-202013298	**Use Valid Value Range for Configuring Remote Tags** The valid value range for tags on remote-mirroring VLANs is 1 to 4,094. Use these values for configuring the remote tag in the `enable mirroring` command.
PD3-202013281	**Running the "enable learning" Command on Remote Mirroring VLANs May Cause a Loss of Traffic** Learning is disabled by default on remote mirroring VLANs. Running the `enable learning` command on those VLANs may cause a loss of remote mirrored traffic.
PD3-79867211	**Mirroring Port Should Not be Allowed in Load Sharing in SummitStack Switches** If you create a load sharing group (trunk), then enable mirroring to a port, the software allows you to add the mirroring port to the load sharing group.
PD3-28378521	**Enabling Load Sharing on a Mirrored Port** Enabling load sharing on a port that is being mirrored causes the mirroring to stop.
MPLS	
PD3-208178928	**Adding a Static Route With MPLS LSP** Adding a static route with an MPLS LSP may cause one of the following problems: • If a static route is added with an MPLS LSP whose transport setting is "IP traffic deny," the route is displayed with an invalid nexthop in the `show iproute mpls` command output. • When a static route is added with an MPLS LSP that is not present in `show iproute mpls` command output. For example, if there are 17 RSVP-TE LSPs to the same destination, only 16 LSPs are eligible for carrying traffic because of a maximum ECMP path limit of 16. Adding static routes with 17 LSPs results in the same observation.
PD3-157687121	**Control Channel Type Router Alert Label Not Found in VCCV Packets** ExtremeXOS software uses Control Channel Type 2 to indicate router alert label mode. In MPLS Router Alert Label mode, VCCV packets are encapsulated in a label stack. However, the existing VCCV packets are sent like a stack without any PW label.
PD3-184989177	**Enabling "LDP advertise static all" Removes Ingress LSPs Using Static Routes** When an `LDP advertise static` setting is set to `all`, all static routes are treated as egress routes and egress LSPs are created. That is, a label is generated and advertised for the static route. If the router at the end of the static route advertises a label matching that static route, the LSP that was previously an egress LSP becomes a transit LSP. An ingress LSP should also be created whenever a label is received, however, the ingress LSP is never created. **Workaround:** Do not use the `LDP advertise static all` configuration in situations where an ingress LSP for a static route is required.
PD3-202184409	**Adding/Deleting a LAG Sharing Port Changes the VLAN Status** Adding/deleting a LAG sharing port changes the VLAN status, which is causing an OSPF/MPLS reconvergence.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-139423053	**RSVP-TE: LSP Summary Statistics Take Excessive Time to Calculate** Running the `show mpls rsvp-te lsp summary` command on a system configured with 2,000 ingress LSPs takes an excessive amount of time to process.
PD3-121985381	**Packets Larger than Configured Jumbo Frame Size are Forwarded** You cannot configure an IP MTU that is greater than the configured jumbo frame size. However, when the jumbo frame size is configured using a smaller value than the IP MTU, the configuration is accepted and the traffic is forwarded using the larger packet sizes.
PD3-118914021	**Label Not Advertised for a Default Route in a Stub Area** When an OSPF neighbor is configured between two LSRs and MPLS, and an LDP session is configured between them, the ABR router advertises a default route to the internal router. The default route is not mapped to a label in the internal router because the ABR does not advertise the label
PD3-97057691	**Mirrored RSVP Path Message Packets have Incorrect IP Header Checksums** When creating a mirrored port and viewing all traffic on a BlackDiamond 10808, the RSVP path packets have incorrect checksums. These path messages occur on egress traffic from the BlackDiamond 10808.
PD3-109748431	**"show tech" Command Shows Erroneous MPLS CLI on a Non-MPLS License System** The `show tech` command shows erroneous MPLS CLI on a non-MPLS license system running on a BlackDiamond 10808. MPLS should determine if the system is MPLS licensed and only then show the CLI.
PD3-188594038, PD3-133340423	**LDP Adjacency Breaks after Enabling PHP Feature** The PHP feature will not work correctly and may break LDP adjacency with its neighbors. Currently, there is no workaround.
PD3-99318269	**"show mpls rsvp-te lsp detail" Command may Not Show Error Condition** If the transmit bandwidth between two RSVP-TE neighbors is sufficient for a given LSP, but the receive bandwidth is not, the LSP does not come up. The reason for the error is not displayed in the `show mpls rsvp-te lsp detail` output.
PD3-92653036	**Egress LSPs using Advertised Implicit NULL Labels are Not Displayed** The `show mpls label`, `show mpls rsvp-te label`, and `show mpls rsvp-te lsp` command output currently does not display egress LSPs using advertised implicit NULL labels.
PD3-111544904	**Explicit NULL Labels are Treated as Implicit NULL Labels** When a router receives an explicit NULL label, it is incorrectly treated as an implicit NULL label, so rather than sending label 0, no label is sent.
PD3-93218551	**Packets with Router Alert Label (0x00001) are Not being Forwarded** If either an egress or a transit LSP traverses the system, and an MPLS labelled packet containing a router alert label is received, that packet is not forwarded.
PD3-93069318	**VLANs Configured as Protocol "any" Should be Added to MPLS** Only VLANs configured as protocol any should be added to MPLS.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-104731701	**ExtremeXOS Does Not Send Back ICMP Responses for Traceroute through Non-Pipe Mode LSPs** When a traceroute is performed by setting the MPLS TTL to the IP TTL, ExtremeXOS does not correctly send back an ICMP response. The result is "*" characters in the traceroute for the routers that timed out. If a route is available, ExtremeXOS should attempt to send back an ICMP response.
PD3-93630853	**LDP Should Not Advertise Certain Label Mappings** LDP should not advertise a label mapping for a direct VLAN that does not have IP forwarding enabled.
MPLS	
PD3-204793983	**Egress Rate-Limit is Not Accurate in "show port utilization" Command Output** The egress rate-limit shown in the command output of the `show port utilization` command is not correct.
PD3-203917264	**Changing Explicit Route Object of LSP Does Not Clearly Show LSP Status** When an explicit route object (ERO) is changed for an LSP session that is up, the LSP that is already up is not torn down. LSP stays up based on the older values. The retry count continues to increment as LSP tries to come up with new values by querying routes every 30 seconds. This is done while the earlier LSP session is still active using the previously configured values. See the retry count in the command output for the `show mpls rsvp-te lsp <lsp_name> detail` command.
Multicast	
PD4-339945634	**Packets Ingressing on a Member of a Load-Sharing Group in the Mirrored VLAN Should be Mirrored** When a load-sharing group is a member of a mirrored VLAN, packets ingressing on the member of the load-sharing group in the mirrored VLAN should be mirrored. On the Summit family of switches and BlackDiamond 8800 modules, packets ingressing on member ports other than the master port of the load-sharing group in the VLAN are not mirrored. **Workaround:** Packets ingressing non-master ports in the load sharing group on the mirrored VLAN can be mirrored by adding virtual port mirroring filters for each of the non-master member ports.
PD3-203759919	**When Disabling and Enabling MSDP, the Peers Do Not Come up** After disabling and enabling Multicast Source Discovery Protocol (MSDP), the peers do not come up. **Workaround:** Run the `disable msdp` command followed by the `enable msdp` command.
PD4-318846862	**L3 Multicast Traffic in a VPLS vMAN is Forwarded Twice When the LSP is Changed** L3 multicast traffic in a Virtual Private LAN Services (VPLS) vMAN is forwarded twice when the Label Switched Path (LSP) is changed to port sharing and is then changed back.
PD4-235071630	**Direct Routes Are Not Stored in the Multicast Routing Table** Direct routes are not stored in the multicast routing table, which may cause problems processing anycast rendezvous points (RPs).
PD3-128093864	**MSDP SA Responses from non-RPF Peers are Not Processed** MSDP Source-Active responses received from non-RPF peers are not processed.
PD3-188594038	**IP Traffic is Not Sent Across MPLS PHP Network** IP traffic is not transmitted across an MPLS PHP enabled network.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-189399801	**"show pim rp-set" Command Does Not Always Show All Rendezvous Points** The command output for the `show pim rp-set` command does not always show all the Rendezvous Points for a multicast group. **Workaround:** Do not configure the group address in the rp-list with a non-zero host portion.
PD3-200659931	**Traffic May Take 210 Seconds to Recover After a Failover** In a worst case scenario, after a failover, traffic may take 210 seconds to recover on a switch with a PIM DM configuration.
PD3-78144711	**"show ipstats" Command Does Not Increment IGMPv3 Statistics** The `show ipstats` command does not increment IGMPv3 statistics.
PD3-79383551	**IGMPv3 Report Record Type "5" Message Does Not Work Correctly** IGMPv3 Report Record type "5" does not work as expected when sent after a type "2" or a type "4" message.
PD3-2841008	**Multicast Packets Getting Dropped when Sent at Line Rate** With PIM, when small-sized multicast streams are ingressed at line rate, there is an initial packet drop of 50% to 70%. This is seen on BlackDiamond 8800 and Summit X450 switches.
PD3-139683642, PD3-16451411	**"show pim" Command Only Counts Null-Registers** The output of the `show pim` command displays the cumulative counter for the PIM register in/out and the register-stop in/out. When the ExtremeXOS switch is a first-hop router, it sends out the real register first. After a particular mroute has been established, PIM then periodically sends the null-register. The "Register out" field does not count real registers; it only counts null-registers.
Network Services	
PD3-166858162	**Second Combo Port Does Not Come After Reboot if First Combo Port is Redundant to Another Port** On a Summit X250e-24x switch, if one of the combo ports is redundant to a front panel port, after rebooting, the second combo port does not come up if the primary port for the SRP is active.
PD3-93829391	**Configurations Using VR-Mgmt Interface as RADIUS Client IP Do Not Load** Configurations using a VR-Mgmt interface as a RADIUS client IP may not load at boot-up. However, using an interface in VR-Default will load correctly.

PD3-67431351	**Ingress Rate Limiting and Egress Rate Limiting are Mapping to Multiple Ports**
	Configuring an ingress traffic queue and an egress traffic queue association to multiple ports in sequential order generates the following error:
	`Egress queue already associated to this ingress queue`
	`Configuration failed on backup MSM, command execution aborted!`

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description

PD3-67727590	**vMAN ID ACL Translations May Fail with Transmit Errors**
	Creating two sets of vMAN ACLs with 4,000 entries each and performing a vMAN ID translation on each ACL may generate the following error:
	`.....03/15/2006 17:57:28.84 <Info:pm.config.openingFile> MSM-B: Loading policy RLL20k from file /config/RLL20k.pol`
	`...03/15/2006 17:57:32.46 <Info:pm.config.loaded> MSM-B: Loaded Policy: RLL20k number of entries 4002`
	`.........Error in alloc txmi txmi 0x9f2 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f4 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x1102 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f6 txmdi 0xffffffff`
	`Error in alloc txmi txmi 0x9f8 txmdi 0xffffffff`

PD3-62778911	**Converging MVR with EAPS on a BlackDiamond 8800 Causes a Large Packet Loss** With MVR enabled on a BlackDiamond 8800, when the ingress port is on the egress-list this causes a high volume of traffic loss.
PD3-64743301	**Configuring a Meter Value Not Working Properly on a BlackDiamond 12804** When configuring a meter value using a large number, for example, 10,000 Gbps, on a BlackDiamond 12804 switch the CLI accepts the command. However, when you run the `show meter` command, an incorrect value is displayed.
OSPF	
PD4-299382986, PD4-217017923	**Actual Inter-Area Route is Also Shown in Summary Route** When running the `show iproute` command, the actual inter-area route is also shown in the summary route with a virtual link in the command output.
PD3-133427241	**OSPF Filter Not Filtering All Routes** When an OSPF external filter is configured to deny routes, not all routes are being filtered.
QoS	
PD4-259174051	**Denial of Service Protection Statistics Are Not Cleared** The `clear counters` command does not clear dos-protect statistics.
PD3-202190332	**HQoS Allows Multiple Egress Queues to be Linked to a Single Ingress "allow-egress" Queue** Configuring HQoS allows multiple egress queues to be linked to a single ingress allow-egress queue.
PD3-129177287	**If IRL-ERL Traffic Queue Mapping Extends to all Ports, Port Selection is Void** Create an ingress traffic-queue with `allow egress shaping` and create an egress traffic-queue. Map the IRL to ERL on all ports. Send unidirectional traffic, which should hit the IRL rule at ingress. The same traffic is visible to the ERL at the egress port without selecting the designated port of VLAN/vMAN.
PD3-16578296	**Disabling Load Sharing or Deleting Member Ports from a Trunk** The member ports of a trunk will retain the QoS profile configuration of the trunk (based on the master port) after load sharing is disabled, or if a port is removed from the trunk.
RMON	
PD3-12950492	**"clear counter" Command Not Supported** Issuing the `clear counter` command might cause a high number to be displayed in variables such as etherHistoryOctets, etherHistoryPkts, and etherHistoryTable.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
ScreenPlay	
PD3-204766394	**Discrepancy Between ExtremeXOS CLI and ScreenPlay When Configuring Port Speed and Duplex Settings** There is a discrepancy between the ExtremeXOS CLI and ScreenPlay when configuring port speed and duplex settings. Using ExtremeXOS, you can configure a preferred speed, for example, 1,000, and enable autonegotiation for the duplex settings. Using ScreenPlay, you can only enable or disable autonegotiation without configuring a preferred speed.
PD3-111344472	**Cannot Enable DHCP using WebUI** ScreenPlay allows you to configure DHCP but you cannot enable DHCP.
Security	
PD3-205012219	**Source IP Lockdown Dynamic Deny ACL Counter Not Working Properly** A source-ip-lockdown dynamic deny acl counter is not working properly and increments valid traffic from a trusted client.
PD3-186939931	**Ingress Mirroring is Not Working for DHCP Snooping When Snooping is Enabled** Ingress mirroring is not working for DHCP snooping when snooping is enabled on BlackDiamond 12800 series switches. DHCP snooping works correctly when DHCP snooping is disabled.
PD3-133763260	**New Backup MSM Reboots Twice after Failover** A new backup MSM reboots twice after failover (`run MSM-failover`). The backup MSM initially comes up correctly but is not in the "In SYNC" state. The MSM then reboots without a core and comes up "In Sync" on a BlackDiamond 8800. This problem does not occur consistently and should not affect data transmission. It is recommended that you disable the notify function in the `disable ip-security anomaly-protection notify <log | cache | snmp>` command to avoid potential problems.
PD3-96212671	**DHCP Packets are Not Relayed if "dhcp-snooping violation-action" is Set to None** When DHCP snooping is enabled on a port in a VLAN in monitoring only mode (that is, with the violation-action option set to none) and the switch is acting as a BOOTP relay, DHCP packets are not relayed from the DHCP server on that port. As a workaround, the port can be configured as a trusted-port (trusted for DHCP server packets) with DHCP snooping enabled with a violation-action of drop-packet instead of none. This works the same as setting the violation-action to none viz. The DHCP bindings database is built up by monitoring DHCP traffic but no rogue DHCP server traffic on that port is dropped.
PD3-75120608	**Unconfigure RADIUS and TACACS Does Not Reset Timeout Value to System Default** The `unconfigure radius` and `unconfigure tacacs` commands do not reset the timeout value to the system default of 3 seconds.
PD3-74708933	**RADIUS Authentication Do Not Work Correctly if Console Accesses the Backup MSM** If you are configuring a BlackDiamond 10808 or BlackDiamond 8800 with RADIUS authentication, when telnet or console access is through the master MSM, RADIUS authentication works correctly. However, if console access is through the backup MSM, RADIUS authentication does not work correctly and generates the following error message: `<Erro:AAA.RADIUS.serverNotInit> MSM-B: Authentication server for Switch Management is not initialized`

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-29948301	**Changing a Password after Password Expiration Terminates SSH Session** When a local user password expires, logging into the switch using SSH will prompt you to change your password. After changing the password, the current SSH session will be terminated and you will need to login to the switch using the new password.
sFlow	
PD3-205380274	**sFlow Does Not Work in BVLANs and SVLANs** sFlow is not working on ports that are included in BVLANs, SVLANs, and occasionally vMANs. sFlow can be enabled and configured for ports in BVLANs, SVLANs, and vMANs, but nothing is sent to the sFlow collector.
SNMP	
PD3-206632121	**SNMP Query for extremePortQosStatsTable OID Returns a Value of 0** On a Summit X450a series switch, running an SNMP query for the extremePortQosStatsTable object identifier returns a value of 0. This should return the actual number of packets counted.
PD3-181304741	**entPhysicalDescr MIB for XENPAK Modules Always Shown as XGM-** After inserting a XENPAK in a stack (XGM2-2xn, XGM-2xn) and performing an snmpwalk on the entityMib entPhysicalDescr variable, XGM- is always shown, not the complete module description.
PD3-39411271	**icmpInMsgs Counter Displays only Incoming ICMP Packets** icmpInMsgs counter will display the incoming ICMP packets for VR-Default only.
Spanning Tree Protocol	
PD4-292225290	**STP BPDUs are Generated When Connecting MSTP Configured Switch to Another Switch** A large number of Spanning Tree Protocol (STP) BPDUs are generated when an MSTP configured switch is connected to another switch that is using a default configuration.
PD3-189927343	**Temporary Loop Occurs When a Root Bridge is Taken Down** A temporary loop occurs when a root bridge is taken down by disabling all ports or powering down the switch.
Stacking	
PD3-136493921	**AAA Services Do Not Become Available on Stacking Switch that has a Mismatched License** If a switch is added to a stack whose master switch has a license level that is greater than the level of the switch, the switch will fail. The complete condition can be seen using the `show slot detail` command. In this state, the switch does not have AAA services available. You will only be able to log into the switch using the failsafe account that was last assigned to it. You must log into the switch to upgrade the license. If the switch is not using the failsafe account configured on the stack, you can use the `synchronize stacking {node-address <node-address> | slot <slot-number>}` command to copy the failsafe account information from the master switch to the failed switch NVRAM. You can also use the `configure stacking license-level` command to configure a license level restriction on the entire stack and then reboot the stack. Once the stack is restarted, there is no longer a license mismatch, enabling you to log into the switch and upgrade the license. From the master switch, run the `unconfigure stacking license-level` command to get the stack to operate at the desired license and then reboot the stack.

Table 32: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-126650411	**Stackable Systems with Two or More Nodes may Experience Random VRRP Master/Backup Flapping** A stackable system with two or more nodes may experience random VRRP master/backup flapping issues after an MSM failover when configured with the maximum 128 VRRP instances using the minimum advertisement interval of 100ms and maximum tracking entries.
System Related	

PD3-28577971	**Show Log Error Messages**
	Messages stored in NVRAM are in encoded format. To restore the ASCII text of a message, the version of ExtremeXOS loaded must be able to interpret the data written prior to reboot. When the encoded format for a particular message cannot be interpreted by the version of ExtremeXOS currently loaded, the messages are displayed in the following format.
	`03/21/2005 17:15:37.36 <UNKNW:epm.28>: NO MESSAGE DECODE; Missing component "epm" v24.2`
	`DUMP-00: 00 2C 00 01 FF FF FF FF 00 00 00 95 42 3F 71 B9 '.,..........B?q.'`
	`DUMP-10: 00 14 C3 C1 00 11 00 1C 01 FF 00 08 65 70 6D 00 '............epm.'`
	`DUMP-20: 08 FF 00 0C 00 18 00 02 65 70 6D 00 '........epm.'`

VRRP	
PD3-202801091	**VRRP Master Accepting Packets Addressed to a Virtual IP Address** A VRRP master should not accept or respond to packets addressed to a virtual IP address associated with a virtual router if the master is not the IP address owner.
WAN PHY	
PD3-101226461	**WAN PHY "show" Commands Should Not be Applied to non WAN PHY Ports** When `show wan-phy` commands are run on non WAN PHY ports, the ports display the headers. It should only display the error `wan command is not supported on non-wanphy port 25`.

Known Behaviors

The following are limitations in ExtremeXOS system architecture that will not be resolved.

Table 33: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-995543551	When configuring an ip-mtu as 9,216, the value is reduced to 9,194 after upgrading to ExtremeXOS 12.1 or later.
PD4-440122302	Log messages should not be flooded when an ARP violation occurs, which is causing the EMS server to be busy.
PD4-765092558	When RADIUS authentication for a MAC-based network login IP address fails, a UPM profile generates a warning message.

Table 33: Platform-Specific and Feature PDs (Continued)

PD Number	Description
PD3-197435644	LACP with address-based algorithms on L2 links is sending multicast traffic on multiple links.
PD3-204022938	If a MAC move occurs in an isolated subscriber VLAN without the link of the port going down, the MAC address is not learned on the new port.
PD3-182634820	The thttpd process cannot be restarted using the `start process` or `restart process` commands after the process exits preceded by a "Thread thttpd ID does not respond" log message.
PD3-203517161	In a network where a BlackDiamond 8800 or a Summit X450 switch is forwarding packets, occasional packet drop is observed on certain egress ports.
BlackDiamond 8800 Series Switch	
PD4-832478607	On BlackDiamond 8800 series switches, when a port belongs to two different VRRP instances with the same VRID, and one of the instances is a master VRID and the other a standby VRID, broadcast packets belonging to the standby VRRP VLAN generated by the master VRRP in that VLAN are not forwarded.
BlackDiamond 10808 Switch	
PD3-175604157	A BlackDiamond 10808 switch with a dual speed copper/fiber SFP shows a link as active even though a cable is not connected.
BlackDiamond 12800 Series Switches	
PD4-580590984	Meters cannot be disassociated from HQoS queues that are in use. HQoS queues must first be removed before associated meters can be deleted.
PD3-206766987	Hitless upgrade is not supported for network login when upgrading from a previous version of ExtremeXOS software to ExtremeXOS 12.1. If you attempt to perform a hitless upgrade, all existing clients must be reauthenticated after a failover. Error messages such as `genesisNetLoginHandleGet: Port 0x08 NOT found`, may be shown on the console and the system log. If a hitless upgrade is required, it is recommended that you globally disable network login and re-enable it when the upgrade is complete.
PD3-131941899	Disabling and enabling a GM-20XT I/O module twice causes the slot to enter the Failed state and displays the following error message. `Error Generic Error(-1) from HAL on CardExec POWER_OFF(10) for slot 1`
Summit Family Switches	
PD4-309137281	During an ExtremeXOS software upgrade, the following message may be seen when a Summit switch contains a large number of VLANs: `08/14/2008 17:12:06.56 < Crit:HAL.Sys.Critical > Switch low on Memory.` When the upgrade is complete, the system reboots. The saved configuration remains intact and is restored using the new ExtremeXOS image.
PD3-168702411	On a Summit X250e-24x, when a link is connected to an SX SFP mini-GBIC on one side and a 100 FX on the other side of the link, the link is shown as being up on the 100 FX side but the link is down on the SX side.

Table 33: Platform-Specific and Feature PDs (Continued)

PD Number	Description
ACL	

PD4-613216219	The following error message is seen when applying `all_vlan` to 70 or more VLANs.
	`* SummitX450a-24x.83 # configure access-list all_vlan vlan sh241_vlan`
	`Error: ACL install operation failed - meter hardware full for port 1`

PD3-202962401, PD3-88458683	If you run the `clear ipmc fdb` command, initially some multicast packets are forwarded in slowpath. Those slowpath forwarded multicast packets are being denied by ACL.
PD3-76416480	When an egress ACL is used to deny vMAN traffic with unknown unicast, multicast, and broadcast destination addresses, the egress ACL cannot deny the traffic.
PD3-208402260	If you create a telnet access-profile using the destination-address match statement, the destination-address statement is not evaluated. Other match statements within the entry are evaluated. If there are no other statements, then the action is taken regardless of whether the destination-address is a match.
PD3-135380560, PD3-134870425	For Summit X450 and BlackDiamond 8800 switches, installing, unconfiguring, and refreshing a large number of static or dynamic ACL rules with meters may take a long time. **Workaround:** Install ACL rules with meters in the order "higher precedence first," and uninstall ACL rules with meters in the order of "lower precedence first."
PD3-208751163	MSM-B reboots when applying 20,000 ACL rules with 20,000 ingress queues.
PD3-135200936	When an ACL policy file containing meters associated with ACL rules is applied to a port, the system should verify that the meters are present before installing the ACL policy file. If meters are not present, the system should generate an appropriate error message and the ACL policy file should not be installed.
PD3-121018177	Action redirect-port is not supported on egress ports. Even if redirect is applied to an egress port, while redirect-port has no effect on egress traffic, the counter should work correctly.
PD3-27536111	When you edit tcpDestPort.pol using the VI editor and save it with a different filename, the new file is not applied.
BGP	
PD4-1243359825, PD4-1185696661	A BGP process crash with signal 11 occurs when disabling and enabling a BGP peer with 15,000 routes.
CLEAR-Flow	
PD3-16311713	A syntax error is not displayed when a policy file is configured using CLEAR-Flow rules on BlackDiamond 8800, BlackDiamond 8806, and Summit X450 switches. The rule is silently ignored.
Control Protocols	
PD3-160517465	Configuring EAPS and MSTP on the same port for the same VLAN results in a longer convergence time for the EAPS topology change. Even after a RxPduRingUpFlush is triggered for the topology change, the FDB entry is cleared.
EAPS	
PD4-716385097	An EAPS controller goes into a blocking state even when a ring is not complete.

Table 33: Platform-Specific and Feature PDs (Continued)

PD Number	Description
IP Routing Products	

PD3-188555286	Not all shared static IP routes may be utilized following a link flap to one or more gateways used by those static routes. For better resiliency when sharing static routes, configure static ARP and FDB entries for each gateway used by the shared static routes. To do this, run the following commands for each gateway:
	`configure iparp add <ip_addr> {vr <vr_name>} <mac>`
	`create fdbentry <mac_addr> vlan <vlan_name> ports <port_list>`
	This affects BlackDiamond 8800 series and Summit X450 a-series and X450 e-series switches only.

PD3-161152153	A switch experiences high CPU usage and logs an error message when running a RIP process when an snmpwalk is performed even though RIP is globally disabled: `07/12/2007 19:47:43.10 <Info:EPM.cpu> MSM-A: CPU utilization monitor: process rip consumes 99 % CPU`
PD3-154525838	A BlackDiamond 8800 switch with a 10G4X module, or a Summit X450 switch with an XGM 10 Gigabit module, may drop/duplicate/loopback packets on 10 Gigabit ports when PIM is enabled while load sharing is configured and IP multicast is present.
IP Unicast	
PD3-192315271, PD3-182815070	When a switch is configured for proxy ARP with the `always` keyword, the switch will not respond to a gratuitous ARP request, it will only respond to ARP requests.
IS-IS	
PD3-206929752	The ExtremeXOS implementation of IS-IS supports draft-ietf-isis-restart-02. As a result, IS-IS graceful restart vendor interoperability is limited to devices that support draft-ietf-isis-restart-03 or earlier.
Mirroring	
PD3-208247531	A BlackDiamond 12800 switch cannot mirror more than 2G of traffic for egress mirroring. Doing so may be cause RX errors and the switch to reboot. This is a hardware limitation for the BlackDiamond 12800 switch for egress mirroring.
MPLS	
PD3-210216393	When configuring a service vMAN to share a port with a service VLAN, the L3 multicast on the service VLAN is not forwarded by VPLS. Forwarding multicast traffic from the service VLAN works correctly.
Multicast	
PD3-207976461	Counters are not getting updated on ingress and egress node transport LSPs when sending traffic by way of VPLS. The counters are being updated on the transit node only. This problem occurs on all three transport LSPs (static, RSVP, and LDP).
PD3-192434331	The switch does not allow a user to create a static ECMP multicast route when the `protocol` option is included in the `configure ipmroute add` command. An error message is displayed stating that the multicast route already exists.
Network Login	
PD4-780622490	When a MAC-based network login user logs out, the UPM profile configured for the user's unauthentication is not executed.
PD3-167032424	A network login authentication web session terminates after a session refresh times out when moving to a nonexistent VLAN.
Policy Manager	
PD3-29818741	ETHER-P-8021Q is not a valid ethernet-type match criteria and generates a syntax error. You can use 0x8100.

Table 33: Platform-Specific and Feature PDs (Continued)

PD Number	Description
Security	
PD3-75465301	The `unconfigure radius` command does not clear the RADIUS authentication and accounting counters.
SNMP	
PD3-204276011	An SNMP get request to query an FDB sequence number in the ExtremeFdbMacFdb MIB is not returning a fixed value.
PD4-634374697	If a permanent SNMP community is deleted using an earlier software release, those entries are not present even after the upgrade to ExtremeXOS software,which does not support deleting permanet SNMP community entries.
SSH and SSH2	
PD3-20944751, PD3-14620801	After regenerating the SSH key you must save the configuration and then terminate SSH. Terminate the SSH process using the `terminate process exsshd graceful` command and then restart the process using the `start process exsshd` command.
Stacking	
PD3-138014104	You can run the `reboot stack-topology` command on any stacking switch while the master switch is downloading or installing an image, or saving a configuration file. This results in incomplete file operations before the reboot takes place, which may render the image or configuration unusable. Be sure that neither operation is in progress when rebooting the stack.
PD3-133978700, PD3-138140417, PD3-137976136	If you remove and quickly replace the stacking cable causing a separation of one or more switches from the stack, the stack master may not consistently detect the missing slots. The system may try to reinitialize the slots without first performing the necessary reboot. Extreme Networks recommends that you wait at least five seconds between removing the cable and replacing it again.
PD3-119233421	VLANs can only be created if there is at least 20MB of main memory available. A port can only be added to a VLAN if there is at least 30MB of memory available. Currently, one of these limits will be encountered if approximately 2,500 VLANs with eight ports each are configured evenly. Changing the order in which VLANs are created and ports are added may result in different configurations at the time a limit is encountered. Also, since memory is shared with other features, for example, route tables, the number of VLANs and ports that can be created may be considerably lower.

Resolved Issues in ExtremeXOS 12.1.4-patch1-9

The following issues were resolved in ExtremeXOS 12.1.4-patch1-9. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 34: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-812156545	The CLI command "show fdb <name of the private vlan>" output loops for specific MAC addresses.
PD4-1142795450	In some cases, EXOS CLI allows load sharing group to be formed using ports with different link speeds.
PD4-935914533	Getting inconsistent "Destination Host Unreachable" return in the ping test to a local, but non-existing host.
BlackDiamond 8800 Switch	
PD4-805462597	A slot fails on a BlackDiamond 8800 series switch when enabling dot1p examination inner-tag ports on more than 24 ports in a vMAN.
BlackDiamond 10808 Switch	
PD4-1108500108	In some cases, CLEAR-Flow delta rule triggers while not needed on backup MSM.
IP Routing Protocols	
PD4-1231117748	In RIP, Output route policy is applied to Input route policy internally after changing and refreshing Output route policy file.

Resolved Issues in ExtremeXOS 12.1.4-patch1-8

The following issues were resolved in ExtremeXOS 12.1.4-patch1-8. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 35: Platform-Specific and Feature PDs

PD Number	Description
BlackDiamond 10808	
PD4-1372389633	With PIM snooping enabled on a pure L2 VLAN, PIM snooping entries timeout without being refreshed, even though PIM hello packets are received on the VLAN port. This behaviour is only seen after a BlackDiamond 10808 switch fails over to MSM-B and MSM-A becomes the slave switch.

Resolved Issues in ExtremeXOS 12.1.4-patch1-7

The following issues were resolved in ExtremeXOS 12.1.4-patch1-7. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 36: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-828470206	The invalid syntax keyword `tag_name` is added when configuring a syslog target.
BlackDiamond 10808 Switch	
PD4-804225168	ESMI related warning messages are seen in the output of the `show log` command whenever an SSL certificate with a key length of 4,096 is created or the HTTPD process is restarted.
ACL	
PD4-1027427745	The ACL action modifier "log" does not work with IGMP ACL.
PD4-1027427581	For ACL counters for IGMP message type, the direct offset is calculated and the protocol type in the IP header is not checked. Therefore, any IP datagram matching the offset is counted as matching. **Workaround:** Set a "protocol igmp" match condition explicitly in the policy file.

Resolved Issues in ExtremeXOS 12.1.4-patch1-6

The following issues were resolved in ExtremeXOS 12.1.4-patch1-6. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 37: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1175951471, PD4-1085211320	VLAN mirroring cannot mirror packets that are ingressing a LAG port when the master port link is disabled.
BlackDiamond 12800 Series Switch	
PD4-1217032435, PD4-1191404997	When disabling and enabling a BGP peer with 15,000 routes multiple times, an assertion failure occurs and the BGP process crashes with signal 6.
PD4-1232462236	A hardware error may occur on a BlackDiamond 12800 series switch resulting in a misread on the backplane SerDes FPGAs. This misread is interpreted by the system-health-check as an error, which in turn may cause an I/O module or MSM to be taken offline.

Resolved Issues in ExtremeXOS 12.1.4-patch1-5

The following issues were resolved in ExtremeXOS 12.1.4-patch1-5. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 38: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1232462178, PD4-1221696686	ExtremeXOS software is unable to upgrade an ExtremeXOS software license to any switch that has a serial number beginning with 0953x-xxxx using the `enable license file <license-file.xlic>` command.
EAPS	
PD3-175211031	The ExtremeXOS CLI does not prevent EAPS health check PDUs from looping using the `permit all` keywords when installing ACLs.

Resolved Issues in ExtremeXOS 12.1.4-patch1-4

The following issues were resolved in ExtremeXOS 12.1.4-patch1-4. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 39: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1171055143, PD4-1156762929	A triggered IGMP query with the wrong 802.1Q tag is sent on a vMAN enabled port.
SNMP	
PD4-1155806081, PD4-935076380	When a switch receives UDP packets with a source port of 3503, memory depletion occurs and the switch may reboot.

Resolved Issues in ExtremeXOS 12.1.4-patch1-3

The following issues were resolved in ExtremeXOS 12.1.4-patch1-3. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 40: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-931823732	A loop occurs after disabling learning on a protected VLAN on an EAPS master. **Workaround:** To stop the loop, disable and enable the EAPS primary port.
PD4-1099203316	Egress vMAN ACLs are not getting matched, even though the traffic matching the ACL match condition is egressing the switch port.
BlackDiamond 8800 Series Switch	

PD4-983957922	After running an MSM failover, the backup MSM shows an asterisk in the command prompt after rebooting the switch. To clear this, save the configuration.
	`RT030101_TEST_LAB.2 >`
	`* RT030101_TEST_LAB.2 > show slot`

Summit Family Switches	
PD4-1155294979, PD4-460349822	On Summit X450 switches, 1 Gigabit links take more time to detect a link down than 100 Mbps links.
DHCP	
PD4-1124676271, PD4-727955846	DHCP OFFER and DHCP ACK packets are duplicated in a VLAN aggregation setup if a DHCP request is received on a subVLAN.
OSPF	
PD4-885811009	Deleting ports and unconfiguring IPv6 adresses on a Summit X450a switch causes an OSPFv3 assertion failure.

Resolved Issues in ExtremeXOS 12.1.4-patch1-2

The following issues were resolved in ExtremeXOS 12.1.4-patch1-2. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 41: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1027500181	The `show tech all detail logto file` command does not complete execution.
PD4-1087700914, PD4-698458422	PIM DM causes higher bandwidth consumption with multicast when no subscribers exist.

Table 41: Platform-Specific and Feature PDs (Continued)

PD Number	Description
General	
IGMP	
PD4-926340897	Even with IGMP proxy enabled, when an IGMP subscriber leaves, the IGMP-leave is forwarded with multiple subscribers on one port.

Resolved Issues in ExtremeXOS 12.1.4-patch1-1

The following issues were resolved in ExtremeXOS 12.1.4-patch1-1. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 42: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-1012121678, PD4-983772991	The ifMauDefaultType MIB is populated with the wrong value when a switch is running ExtremeXOS 12.3.3 software.
PD4-901961135	When an SNTP client is configured, the following log message is displayed every 4,096 seconds: `10.101.1.97: <189> Aug 18 18:31:44 DM: : Setting hwclock time to system time, and broadcasting time Tue Aug 18 19:40:00 2009: 10.101.1.97: <189> Aug 18 19:40:00 DM: : Setting hwclock time to system time, and broadcasting time Tue Aug 18 20:48:16 2009: 10.101.1.97: <189> Aug 18 20:48:16 DM: : Setting hwclock time to system time, and broadcasting time Tue Aug 18 21:56:32 2009:`
PD4-1013258326	An FDB refresh fails on a port when there is active traffic and a link flap on another port on the switch.
PD4-1007713804	Disabling learning on a VLAN, or creating a remote mirroring VLAN, causes excessive flooding.
PD4-1056306414, PD4-679109661	The LLDP process may crash with signal 11 when using the configure lldp port ALL advertise vendor-specific dot1 port-protocol-vlan-id vlan < vlanname > command.
PD4-901582203	The typographical error in the following error message has been corrected: `<Warn:AAA.RADIUS.serverSwitch> MSM-A: Switch to server...`
Summit Family Switches	
PD4-997419038	When dot1x and MAC-based authentication are both enabled on a port and a user is first authenticated using MAC-based authentication, while dot1x authentication is also running, the response from the RADIUS server is dropped.
PD4-986904840	FDB entries are aging out even after receiving packets on the connected port.
Multicast	
PD4-1008069840	Enabling IGMP snooping globally results in an error for remote mirroring VLANs
Network Login	
PD4-464577708	A web-based network login client cannot be authenticated using the URL `http://< switch-ip >/hello` or `http://< switch-ip >/login`.

Table 42: Platform-Specific and Feature PDs (Continued)

PD Number	Description
SNMP	
PD4-902287187	The EXTREME-V2TRAP-MIB definition misses the "EapsRingPort" at the IMPORTS section. Because of this, the Spectrum NMS fails to compile the ExtremeXOS 12.1.3 MIB file with an error against EapsRingPort.

Resolved Issues in ExtremeXOS 12.1.4

The following issues were resolved in ExtremeXOS 12.1.4. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3-patch1-5, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 43: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-899333484	The thttpd process CPU utilization increases and HTTP/HTTPS is not accessible if sock/ stress attack is performed on an HTTPS port. This issue persists indefinitely even after a sock/stress attack is removed.
PD4-924242747	The FDB process may die with signal 11 when the `show fdb statistics` command is executed.
PD4-920567275	Process FDB may die with signal 11 when processing SNMP Get requests for dot1dTpFdbTable.
PD4-767595507	The log filter is not shown in the output of the `show upm profile <profile-name>` command.

PD4-978931780, PD4-975759347	When stacking redundancy and telnet access-profiles are configured, the following error is displayed:
	`Connection refused`
	`Connection closed by foreign host.`

BlackDiamond 12800 Series Switch	
PD4-832095668	The ACL match condition `ports ingress <port-no>` causes incoming packets to be forwarded to all ports in a VLAN as per the VLAN tag for incoming packets, even though the ingress port is not part of that VLAN.
Summit Family Switches	

PD4-816941511	The following error may be seen when a Summit family switch experiences an intermittent interface diagnostics failure when extended diagnostics tests are run multiple times.
	`ERROR: Transmitted 5.44M packets from slot 1 MAC-0 port 45`
	`ERROR: Received 4.01G packets on slot 1 MAC-0 port 45`
	`ERROR: Packets dropped: 4.00G`

PD4-598343155	On a Summit X450 switch, OSPF may not form an adjacency after enabling sFlow.
ACL	
PD4-964769251, PD4-963068135	An ExtremeXOS switch reboots with memory depletion for a 128 memory block while loading a flow-redirect configuration.

Table 43: Platform-Specific and Feature PDs (Continued)

PD4-670315790	When configuring egress ACLs on a load-shared port the following incorrect error message is displayed: `Duplicate ACL config, Note: Egress ACL need be applied on the Master port only`
CLEAR-Flow	
PD4-852494655	With CLEAR-Flow enabled, CLEAR-Flow ACL threads may be killed by EPM.
OSPF	
PD4-929585893, PD4-875793527	Incoming router LSAs with a router link greater than 420, causes the OSPF process to crash with an assertion failure.
PD4-896536108	When running OSPFv3 over a 6-in-4 tunnel interface, OSPFv3 treats the interface as broadcast rather than point-to-point.

Resolved Issues in ExtremeXOS 12.1.3-patch1-9

The following issues were resolved in ExtremeXOS 12.1.3-patch1-9. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 44: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-740925847	The following error message is displayed in the log when adding ports to an ESRP slave VLAN. `<Crit:vlan.err.criticalInfo> MSM-A: Critical Info: sysctlWriteSetting: cannot open file.`
PD4-507170288	Traffic received on an STP/EAPS blocked port is being sent to the CPU if the source MAC address of the incoming packet matches the MAC address of the DUT system.
BlackDiamond 8800 Series Switch	
PD4-791316018	When using SCP to download an image, the image fails to install on the backup MSM and the following error is displayed: `Installing to MSM-BError: Failed to install image - tar: /scratch/bd8800-12.1.3.14.xos: No such file or directory.`
Summit Family Switches	
PD4-814229965	Multicast packets using a system MAC address as a destination MAC address are perodically leaked in slowpath every 30 seconds.
PD4-798967898	A Summit X450 switch shows an error when trying to apply a dynamic ACL using the meter action-modifier.
ACL	
PD4-809832196	The output for the `show configuration acl` command contains the wrong syntax for meter configuration if the `create meter <meter-name>` command has just been executed.

Table 44: Platform-Specific and Feature PDs (Continued)

SNMP	
PD4-888471111	The snmpMaster process experiences memory depletion while sending out AuthFailure SNMP traps. **Workaround:** Disable the AuthenTraps by setting the OID snmpEnableAuthenTraps to value 2 (disabled). `snmpset -v 2c -c snmpEnableAuthenTraps.0 i 2`
PD4-929531697, PD4-923129104	Performing an snmpwalk on a usmUserTag OID (1.3.6.1.4.1.99.12.35) causes the snmpMaster process to die with signal 11. **Workaround:** Run the following command to block the access to that OID and prevent the crash. `configure snmpv3 add mib-view defaultUserView subtree 1.3.6.1.4.1.99.12.35 type excluded`
Spanning Tree Protocol	
PD4-925787371	In RSTP, when a port becomes a root port and an alternate port exists on a bridge, agreement BPDUs are not immediately sent back as per standards.

Resolved Issues in ExtremeXOS 12.1.3-patch1-8

The following issues were resolved in ExtremeXOS 12.1.3-patch1-8. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 45: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-505794657	Repeatedly running multiple commands from a telnet session causes memory depletion in the exsh process.
PD4-791833227	If an IPv6 tunnel is configured, adding a static route causes the Route Table Manager to crash with a signal 11 error.
PD4-767856469	After running the `save` command and rebooting a switch with a VLAN translation configuration, duplicate packets are sent to member VLANs from the translation VLAN.
PD4-862521622	Receiving bootstrap packets with a "Fragment Tag" field set to zero causes memory depletion in the PIM process when processing subsequent bootstrap packets.
BlackDiamond 12800 Series Switch	
PD4-907885458, PD4-907885450	SerDes register values have been corrected for optimum performance.
PD4-852419857	Creating and deleting HQoS queues on a BlackDiamond 12808 results in the following error: `Error: Timeout awaiting Traffic Queue operation.`
PD4-723664780	After performing a hitless upgrade from ExtremeXOS 12.0 or later to ExtremeXOS 12.1 or later, packets are sent to the CPU for L3 switching, even though hardware entries exist for the destination IP.

Table 45: Platform-Specific and Feature PDs (Continued)

Summit Family Switches	
PD4-911150963, PD4-911212165	Changing L3 adjacency between trunked and non-trunked ports causes traffic to be forwarded incorrectly.
SummitStack	
PD4-547591482	Performing an snmpwalk on OID 1.3.6.1.4.1.1916.1.4 (enterprises.extremeAgent.extremePort) on a stack returns the error `No Such Object available on this agent`.
Network Login	
PD4-823485808	Limit-learning does not show the blackhole entries if network login is enabled on the same port.
PD4-765586466	Network login enabled ports are authenticating the switch MAC address in certain loopback configurations.

Resolved Issues in ExtremeXOS 12.1.3-patch1-6

The following issues were resolved in ExtremeXOS 12.1.3-patch1-6. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 46: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-500100211	The "vi" process may crash when performing a cut/copy/paste of text that is larger than 10,492 bytes.
PD4-717931715	After upgrading a PoE capable ExtremeXOS switch from software version ExtremeXOS 11.6 to 12.1, the `show configuration poe` command is not available.
PD4-748079627	The debug log `<Info:thttpd.info> 13 line feeds removed` is not necessary and is shown when configuring a switch with HTTPS.
PD4-539277416	Failsafe account authentication fails when trying to access a switch using SSH by way of a management port
PD4-772840867	An Extreme Networks switch ignores the string "priv_lvl" in a TACACS authorization reply packet.
PD4-694359201	Process cliMaster dies with signal 6 in some cases.
PD4-507170653	Policy files containing 850 entries with flood-groups causes an Extreme Process Manager (EPM) watchdog reboot.
BlackDiamond 8800 Series Switch	
PD4-841184307, PD4-238870391	When STP notifies EAPS that it has flushed an FDB table, EAPS no longer performs an additional FDB flush of the local switch. The additional flush was not necessary and had a side effect of inadvertently unauthenticating netlogin clients on the local switch.
PD4-769156523	The message `MSM-A: Error while saving "psePort"` is displayed when a `save` command is executed after reconfiguring a slot as a G48te2 (PoE) to a G48te2 module.
PD4-767590011	A devmgr process crash may occur when the `show version` command is executed.

Table 46: Platform-Specific and Feature PDs (Continued)

BlackDiamond 12800 Series Switch	
PD4-698686480	Even after a vMAN ethertype is changed using the CLI, packets are egressing out the service vMAN using an older vMAN ethertype.
Summit Family Switches	
PD4-805737496	A Summit X450 switch only supports 511 LPM routes.
SummitStack	
PD4-707855726	The `configure inline-power budget` command is not supported on Summit family and SummitStack switches.
PD4-822468393, PD4-803423872	An overheated SummitStack fails, but the ports remain active and traffic continues to be forwarded.
PD4-788067297	Multicast traffic is not forwarded after rebooting a standby switch in a stack.
ACL	

PD4-369088279	If a dynamic ACL is applied to ingress and egress to two or more interfaces (port or VLAN), the `configure access-list delete all` command does not delete the dynamic ACL from all interfaces.
	Workaround: Manually delete the dynamic ACL from each port or VLAN using one of the following commands:
	`configure access-list delete ping port <port-list>`
	`configure access-list delete ping vlan <vlan-name>`

Multicast	
PD4-803604959, PD4-602286396	When PIM hello packets are received, ports are not detected as router ports. The router port is detected based on the IGMP report received from an IP address, but not on the actual PIM packet.
OSPF	
PD4-759590041	After a port in a VLAN is added to an OSPF area, it takes about four seconds to update a neighboring switch.
PD4-767590126	In a jumbo frame environment, an OSPFv3 neighbor gets stuck at EX_START.
PD4-241726909	If two routers, both reachable from one another, originate functionally equivalent AS external LSAs (same destination, cost, and non-zero forwarding address), the LSA originated by the router having the highest OSPF router ID is used. The router having the lower OSPF router ID can then flush its LSA. However, an ExtremeXOS switch does not purge the functionally equivalent AS external LSA when an Extreme OSPF router ID is lower.
PD4-701099374	Setting the ospfSetTrap OID mib-2.14.16.1.1.0 to 0x0000ffff does not cause OSPF to send out OSPF traps.
QoS	
PD4-512656071	A HAL process crash occurs when HQoS is used with CLEAR-Flow and CLEAR-Flow rules are enabled.
ScreenPlay	
PD4-774800225	ScreenPlay shows the wrong port speed after setting autonegotiation to off and on because the XML API returns the incorrect configuration speed after disabling and enabling autonegotiation.
PD4-552010000	The following message is periodically logged when the Event Log screen is left open in ScreenPlay: `Login passed for user admin through xml (::)`

Table 46: Platform-Specific and Feature PDs (Continued)

SNMP	
PD4-747221911	Changing the storage type of default SNMP objects [Communities/Users/Groups/Access] to "non-volatile" allows the user to delete these default SNMP entities like any other user created entity.
Spanning Tree Protocol	
PD4-863979218, PD4-814770957	An STP topology change triggers EAPS to flush FDBs and send FlushFdb PDUs despite the fact that none of the STP protected VLANs are participating in EAPS.
VRRP	
PD4-861034486, PD4-855539430	When ping-tracking is enabled for VRRP, VRRP performs the failover based on a cumulative ping-track failure instead of consecutive ping-track failures.

Resolved Issues in ExtremeXOS 12.1.3-patch1-4

The following issues were resolved in ExtremeXOS 12.1.3-patch1-4. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 47: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-795451285	After disabling flooding for broadcast traffic, the broadcast traffic originated from the switch is not flooded out.
PD4-701906049	The configured value of the sys-recovery-level resets to the factory default after disabling and enabling an I/O module (G48Xa).
PD4-581257425	An error occurs when loading an ExtremeXOS 12.1 or earlier software configuration file if the banner configuration contains a new line character.
PD4-504813986	In a DNS server, if the RADIUS server IP address is specified as CNAME, that is, Alias, a switch is not able to resolve the IP address correctly.
PD4-684400473	A switch does not generate high CPU utilization log messages after executing the `clear cpu-utilization` command, even if process CPU utilization goes above the threshold value.
PD4-757850297, PD4-630233676	After performing a hitless upgrade, the `show version` command output still shows the old master filename, not the new image. However, the `show switch` command output shows the correct image.
PD4-752699185	Untagged vMANs in a LAG cause tagged vMANs to stop forwarding.

PD4-701099735	When running the `disable/enable sys-health-check slot 2` command on an empty slot, a BlackDiamond 10808 logs the following warnings.
	`# show log`
	`<Info:cli.logLocalCm > MSM-A: serial admin: cle slot 2`
	`<Info:cli.logLocalCmd> MSM-A: serial admin: en slot 2`
	`<Info:cli.logLocalCmd> MSM-A: serial admin: disable slot 2`
	`<Warn:AAA.authFail> MSM-A: Login failed for user admin through telnet (10.255.44.27`
	`)<Warn:HAL.Card.Warning> MSM-A: Function pointer is not initialized. Caller: 0x4832f0 Parm1: 0x2 Parm2: 0x0`

Table 47: Platform-Specific and Feature PDs (Continued)

PD4-688252511	Some hosts are no longer reachable after removing an active MSM-B in a cross module link aggregation setup. **Workaround:** Disable and re-enable the load-shared port.
PD4-752568607, PD3-184290391	An initialization error causes an invalid IPML peer to be used on the initial call to dsGetEntryByAttr().
PD4-541064246	When configuring rate-limiting on a switch, the max-burst-size value is not reset after reconfiguring the switch.
PD4-699307521	When running the `show ports stack-ports rxerrors` command, the "RX Over" count continuously increments, even without user traffic.
PD4-759415981, PD4-489103037	A HAL crash occurs when both links of a stack master are disabled.
PD4-759590070	After running the `configure sys-recovery-level slot 1 shutdown` command, the message `Errors will cause Slot-1 shutdown` is displayed on the console and in the system log after then running the `show configuration` or `save configuration` commands.
SummitStack	
PD4-623659132	After a SummitStack failover, the new master node is not reachable using an alternate IP address or gateway.
ACL	
PD4-556797775	The `show access-list meter ports x` command returns all meters on the switch, not just the one associated with `port x`.
PD4-641467077	The telnetd process crashes with signal 11 when the same policy file is used in a telnet access-profile and an ACL.
PD4-738207292	Access-profile configurations for SNMP and SSH modules are not available in the `show configuration` command output.
PD4-667212313	If the `refresh policy` command is invoked by adding more entries to the policy file, then after unconfiguring that specific ACL, an ExtremeXOS switch starts logging messages such as: `Denied packet on ingess interface vlanIf=1000223 slot=1 port=1, too many ACL's & packet rate is too high" and start to drop all the packets received in slow path.`
PD4-757850193, PD4-569838439	Packets that need to be L2 switched are not egressing if the packets hit the IPv4 ACL containing a `redirect` action. This fix requires a regular upgrade on a BlackDiamond 12804 switch. It will not work if you attempt a hitless upgrade on the BlackDiamond 12804 switch.
BGP	
PD4-507188532	When the BGP fast-external-failover feature is enabled, BGP traps such as bgpBackwardTransition and bgpM2BackwardTransition are not generated.
EAPS	
PD4-627092945	When a shared port is configured prior to enabling an EAPS domain, the EAPS protected VLAN does not block the secondary port in some cases.
PD4-682475164	IPv6 neighbor discovery packets sent to the CPU are affecting EAPSv2 PDUs, resulting in the following message: `EAPS Shared Port: Segment timer expired.`
ESRP	
PD4-631761683	When ESRP is disabled, clients using an ESRP virtual IP address as a default gateway are not able to communicate outside the VLAN.

Table 47: Platform-Specific and Feature PDs (Continued)

Network Login	
PD4-684538103	Running the `save configuration` command causes a memory leak in the netlogin process.
PD4-731628986	When rebooting a switch, no local authentication takes place if the authentication order is RADIUS_LOCAL and RADIUS is not reachable.
OSPF	
PD4-707855673	OSPF stops translating external routes after deleting a static route to the same destination IP address.
SNMP	
PD4-713364618	The extremePortVlanStatsTable definition in the EXTREME-VLAN-MIB does not comply with RFC 2578.
VRRP	
PD4-799835165	System memory is depleted when non-ICMP IP packets are sent to a VRRP virtual IP address.
PD4-629585032	VRRP backup does not return the real IP address of the VRRP master for the SNMP object vrrpOperMasterIpAddr.

Resolved Issues in ExtremeXOS 12.1.3-patch1-2

The following issues were resolved in ExtremeXOS 12.1.3-patch1-2. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 48: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-733283307, PD3-209497034	Packets ingressing a BlackDiamond 10800 or 12800 series switch with a multicast destination MAC address and a unicast destination IP address are being dropped.
PD4-602948121	The default value for the CPU monitoring threshold value shown in the CLI help message is different from the default value in the configuration file.
PD4-479342731	In some cases, a redundant port does not go down even though the primary port is up.
PD4-707271073, PD4-615043961	When uninstalling an SSH image, the message `This image will be used only after rebooting the switch!` is displayed.
PD4-732618403, PD4-490976302	The CLI command `show vlan <vlan name> security` does not display output if the VLAN name contains 32 characters.
PD4-732618428, PD4-520283119	The CLI command `configure iparp add proxy` allows an IP address of 0.0.0.0 to be configured.
PD4-728458098, PD4-491202062	Routing protocols such as RIP, VRRP, and PIM cannot be configured on a VLAN if the name of the VLAN contains 32 characters.
PD4-671782473	A PIM process crash with signal 11 occurs when receiving a PIM state refresh packet of type 9.
PD4-496712328	The ExtremeXOS CLI does not display an error message when a user tries to apply a vMAN policy file to an entire vMAN.

Table 48: Platform-Specific and Feature PDs (Continued)

PD4-625406003, PD4-612637671	Process thttpd might die with signal 6 on a switch monitored by EPICenter ScreenPlay.

PD4-731748056, PD3-203116541	The following EEPROM checksum failed error messages may be seen in the syslog:
	`MSM-B card eeprom checksum failed. 0xb8a != 0xb89`
	`MSM-A card eeprom checksum failed. 0xb66 != 0xb65`
	`Backplane eeprom checksum failed. 0xd71 != 0xcd5`

PD4-731748090, PD4-623659557	A non-maskable interrupt occurs while displaying system failure information because of a deadlock in printk.
BlackDiamond 8800 Series Switch	
PD4-702735770	When mirroring is enabled on a BlackDiamond 8800 series switch, some of the incoming unicast ARP reply packets destined for ports on slot 6 (MSM-G8X) are dropped.
ACL	
PD4-666817942, PD4-623943603	When attempting an MSM failover using the `run msm failover` command after an ACL refresh failure, the ACL process dies.
PD4-714733490, PD4-505226018	ACL blackhole entries installed during a refresh policy are not removed if a failover occurs during the refresh policy.
BGP	
PD4-605136780	AS-Path match conditions "_" and "$" may not provide the expected output when using the `show bgp route as-path` command, and when the conditions are used in an ACL. Regular expressions containing multiple "^" symbols do not work.
Multicast	
PD4-676257961	CRC errors are seen in multicast streams in a configuration that has load shared ports with member ports on different slots. This issue is seen when the slot is removed and reinserted.
Network Login	
PD4-690785443, PD4-692471986	When MAC-based network login and MSTP are enabled on a port, the learned FDB is inconsistent.
QoS	
PD4-580590965	Help for the `configure traffic ingress queue q_test add egress queue q_asd ports all` command should be `all ports` instead of `all cos queue`.
sFlow	
PD4-658290001	The `show configuration etmon` command does not display the configured sFlow agent IP address.
SNTP	
PD4-717148757	netTools memory utilization increases if the switch is not able to resolve the server IP address for SNTP.
Spanning Tree Protocol	
PD4-717148940	Intermittent traffic loss is seen in PVST+ configurations.
VRRP	
PD4-713872530, PD4-550811211	With VRRP is enabled on a network VLAN, packets received on subscriber VLANs destined for a VRRP virtual MAC are not getting L3 switched.
PD4-630233727	Configuring VRID authentication using the `configure vrrp vlan vrid authentication simplepassword` command displays the `simplepassword` incorrectly in the output of the `show configuration` command.
PD4-594515501	When enabling VRRP on a superVLAN within a VLAN aggregation, traffic received on the subVLAN (destined for the virtual IP/MAC address) is not getting forwarded through the superVLAN. Instead, the traffic is flooded out the subVLAN ports.

Resolved Issues in ExtremeXOS 12.1.3

The following issues were resolved in ExtremeXOS 12.1.3. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1.3 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.5.3, and ExtremeXOS 12.0.5. For information on those fixes, see the release notes for the specific release.

Table 49: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-256803787, PD3-328904792	On a Summit X450a series switch, software redundant ports work correctly even after multiple link flaps.
PD4-549308147	After uploading an ASCII configuration and then downloading the same conifguration, the configuration changes are not applied properly if the default EAPS hellotime and failtime are modified.
PD4-549927751	Running diagnostics on a slot and then running the `debug hal show sys-health-check` command shows an incorrect `bcmRX ?` message.
PD4-526154880	CLI allows users to specify the vMANs created without using the `learning-domain` keyword as part of the learning-domain action in a policy file.
PD4-488646640	In some instances, vMAN configuration commands are displaying as VLAN configuration commands in the output of the show configuration command. For example, `configure vman vman2 qosprofile QP3` displays as `configure vlan vman2 qosprofile QP3`.
PD4-488295907	For BlackDiamond 8800 and Summit platforms, the ExtremeXOS CLI currently allows using the same vMAN Ethertype for both the primary and the secondary Ethertypes.
PD4-422347775	Interrupting the `ping` command initiated from an ExtremeXOS switch by pressing CTRL+C may cause a "cliMaster" process to crash with signal 11 when a user exits that CLI session.
PD4-453278202, PD4-215198629	If you upgrade a non-active partition on an ExtremeXOS switch, the software automatically moves the pointer to boot from the upgraded image before the image download is complete. If the switch reboots during the upgrade/install, the switch will boot from a corrupt image, resulting in a reboot loop.
PD4-454742273, PD4-415496669	The command output for the `show configuration` command includes `enable vman port` after adding a port to a vMAN, which should not be included in the output.
PD4-463806382, PD4-457878779	Improved switch stability during rapid thrashing of IP ARP cache.
PD4-469891473, PD4-360515775	A loss of traffic occurs when deleting a VLAN translation member VLAN containing loopback ports. **Workaround:** If you change or delete the loopback port, save and reboot the switch, or disable and re-enable the slot.
PD4-469891503, PD4-455932931	Packets are received with an incorrect tag when isolated and non-isolated subscriber VLANs are added to the same port with a loopback port.
PD4-623659410, PD4-623659203	The xml-mode process dies with signal 11 when an "execConfig" XML API request is received.
PD4-505279678, PD4-294938391	A known issue that may result in a MAC FDB polling thread to exit completely (PD3-192633919) without setting the data structure to NULL after freeing memory, causes a switch reboot when the data is accessed from another software thread.
PD4-634581903, PD4-616376561	LACP master ports are removed from a link aggregation group when a stack master is power cycled.

Table 49: Platform-Specific and Feature PDs (Continued)

PD3-204965477	On a BlackDiamond 10808 switch or BlackDiamond 12800 series switches, before loading an ASCII configuration on an unconfigured switch using the `load script` command, delete the ports from the default VLAN using the `configure default delete ports all` command and delete the ports from the default virtual router using the `configure vr vr-default delete ports` <port_list> command.
PD4-445637097	When configuring sampling rates lower than the 256 default value, the show sflow configuration command automatically rounds up the configured sample rate to 256.
BlackDiamond 10800 Switch	
PD4-435982111	A BlackDiamond 10808 series switch may, in some cases, experience the wrong CLEAR-Flow rule trigger and associated actions.
Summit Family Switches	
PD4-572997403, PD4-214435711	When connecting two Summit X450a-24x switches using a dual speed SFP GBIC, after disconnecting the dual speed (100FX/1000LX) SFP receive fiber from one of the switches, the remote port remains active. After disconnecting the dual speed (100FX/1000LX) SFP transmit fiber from the other Summit X450a-24x switch, the local port remains active. See "New FEFI CLI Command" in the feature enhancements section in the "Overview" chapter of this release note.
PD4-683849348	On a SummitStack, IPv4 remote host cache entries are not created after a failover, or if the default stack MAC address is changed manually.
PD4-460847031, PD4-431521921	Rebooting a non-stacking Summit switch may generate the following error: `<Erro:HAL.Port.Error> aspenCardPortLinkscanHandler(): Slot 1, unit 2, HiGig port 24 is not a stack port.`
PD4-562260113	On a Summit X450a stack, the following error message may be displayed in the logs after upgrading the stack: `<Warn:Kern.Card.Warning> Slot-1: shid_eeprom_read:line 3018:I2C I/O operation failed`
ACL	
PD4-438884701	Saving a dynamic ACL fails when using the `permit` or `deny` keywords as the command action.
BGP	
PD4-331422601	A border gateway protocol (BGP) route can point to the wrong next-hop in a route table when a default route is also learned by way of BGP in another scenario.
PD4-490592183	A BGP process crash occurs when a BGP update message is received with an `as-path extended length` flag set.
IGMP	
PD4-415829237, PD3-169760051	Sending an IGMP report on a port with an address reserved for multicast DNS causes the port to become a router port, resulting in all multicast traffic being forwarded on that port in a VLAN.
PD4-646173339, PD4-634273041	When an ExtremeXOS switch receives bursty IP multicast traffic, IGMP snooping entries for some of the multicast streams are not created. Because of this, those IP multicast streams are not egressing the switch, resulting in traffic loss.
Network Login	
PD4-413330044	After a client is authenticated, if the client port is deleted and added back as a tagged port, the client is not authenticated for approximately five minutes. During this time, data traffic from the client is dropped.
PD4-507339161	If the first dot1x login fails, network login remains in an aborted state even after a successful login.
PD4-640023183, PD4-424705571	A switch may stop responding when running the enable netlogin port 3, 4 dot1x command and fail to upload the configuration with the error "Operation draining timed out during save.Setting gCmServer.configCurrent to NULL!!."

Table 49: Platform-Specific and Feature PDs (Continued)

PD4-435524161	A network login client is not moved to an authentication-failure VLAN in specific configurations.
Multicast	
PD4-570383051, PD4-294441183	Some ASCII configuration issues in multicast manager and virtual router modules have been resolved: • Default values for IGMP and multicast listener discovery (MLD) should not be displayed for any user configured virtual routers in the show configuration output. • Disable IGMP and MLD should not display the protocol version in the output of the show configuration command. • Flow VRs will soon be deprecated so disable flowvsr should not be displayed in the output of the show configuration command. • User configured VRs from default configurations can be copied and pasted to other switches with any errors.
PD4-633690679	Multicast manager crashes with signal 11 on hitless upgrade when upgrading from ExtremeXOS 11.6 or 12.0 to ExtremeXOS 12.1.2 or later.
PD4-654813987	When running ExtremeXOS 12.1 or later on a BlackDiamond 8800 a-series, c-series, or e-series switch, or the Summit family switches, you cannot add IP multicast entries. The following error message is displayed when trying to add entries: `Unable to Add IPmc sender entry/Unable to Delete IPmc sender entry`
PD4-308157118	When IGMP snooping is disabled, ingress multicast data packets are not forwarded when vMAN Ethertype is 0x8100. **Workaround:** Set the vMAN Ethertype to default (0x88a8).
Screenplay	
PD4-626440761, PD4-597319891	A memory leak occurs in process “xmld” after a user logs in and logs out of a switch using ScreenPlay.
sFlow	
PD4-446885634	sFlow samples every unicast and multicast packet received on sFlow-enabled ports after CPU throttling sets the sampling rate to a maximum of 536870912.
PD4-486083706	When sFlow is enabled on a port, the incoming Virtual Router Redundancy Protocol (VRRP) announcements on that port are dropped causing dual VRRP masters on the attached switches. The sFlow counters increase when enabled, but the VRRP advertisements do not arrive at the other end.
SNMP	
PD4-453123705	When performing an SNMPwalk for extremeMemoryMonitorSystemTable on MSM-B after an MSM failover, the switch always returns the value set for MSM-A.
PD4-572997662	The SNMP GetNext for the extremeClearflow MIB causes the ACL process to die with a signal 6 error.
Spanning Tree Protocol	
PD4-692156614	Part of an STP configuration is lost when auto-bind and manual port mode are used.
PD4-490740265, PD4-479984841	The command output for the `show configuration stp` command does not show the configured Multiple Spanning Tree Protocol (MSTP) region.
PD4-397626801	STP edge safeguard and network login are supported on the same port.
PD4-451796699	Multiple Spanning Tree Protocol (MSTP) port status changes from "internal" to "boundary" after a switch is rebooted.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-17

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-17. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 50: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-620606253, PD4-576392401	The `upload debug` command returns the error `Error: tftp: The: Unknown host` and the upload fails if the SNMP sysname contains spaces.
PD4-591177208	After executing the CLI command `upload debug`, the EPM process crashes with signal 11, if the SNMP sysname is longer than 15 characters.
PD4-623659052	The extremeFdb MIB entry last-updated field is not updated after adding extremeFdbMacExosFdbTable to the extremeFdb MIB.
PD4-510007350	All traffic ingressing ports on a XM-2HR module that goes to an egress rate limiting queue are being dropped.
Multicast	
PD4-564523051	Multicast traffic shows the incorrect dot1p replacement for CPU (slowpath) forwarded packets.
Spanning Tree Protocol	
PD4-539845558, PD4-558775541	Rapid Spanning Tree Protocol (RSTP) takes more than 4 seconds to forward unicast traffic after performing a topology change.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-15

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-15. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 51: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-576392442, PD4-576392422	Memory usage on data blocks set to "size-128" continues to increase on standby stacking nodes.
PD4-543585023, PD3-121149464	Log timestamps in the `show log` command output now match the time displayed in the `show switch` command output.
PD4-376308672	Packets (other than L2 switched) are egressing with the wrong VLAN tag on the ports in the I/O module that are part of cross-module load share and are hot swapped.
PD4-552244804, PD4-552244726	Removing a master MSM results in a 5-6 second packet loss for port traffic going through the master MSM backplane.
PD4-498613775	A HAL crash with signal 11 error occurs on stacking platforms after running diagnostics on one of the stacking nodes.
PD4-572997711, PD4-471535375	On switches with dual MSMs, when running the `upload debug` command, the EPM process may die with a signal 11 error.
BlackDiamond 12800 Series Switch	
PD4-573244730, PD4-320452728	Running CLI commands on a BlackDiamond 12800 series switch with an MSM-6R module shows an intermittent delay of 30 to 60 seconds during command execution.
PD4-589865012, PD4-456860808	When reinserting a XENPAK module in a BlackDiamond 12800 or 10800 series switch, it may be shown as unsupported.
ACL	
PD4-556568561	L4 access control list (ACL) rules are also being applied to fragmented packets.
PD4-519335296	When hot-swapping an I/O module, a DiffServ configuration does not take affect.
BGP	
PD4-483670239	The $ character is not working as a regex match condition when used in the `show bgp routes as-path` command.
DHCP	
PD4-252386438	A DHCP decline message is not forwarded when IP security is enabled with DHCP snooping.
ESRP	
PD4-295424750	Running ESRP on two switches causes the ESRP domain on one switch to remain in a pre-master state and the neighboring switch to become the master. This issue is seen when active ports are increased on both the master and slave switches at the same time.
SNMP	
PD4-589725036, PD4-526154842	SNMP Get for ipRouteTable (OID 1.3.6.1.2.1.4.21) takes hours to complete when a switch has approximately 260,000 IP routes.
Spanning Tree Protocol	
PD4-603988151	An MSTP revision level cannot be set to a value outside the range 0 to 3. The MSTP revision level can now be set to any value between 0 and 65535.
PD4-587670304	The STP process crashes when changing a link type from "edge" to other types.

Table 51: Platform-Specific and Feature PDs (Continued)

PD4-597477613, PD4-597296541	A link flap of an edge safeguard enabled port causes a switch to generate a "Topology Change" STP BPDU, even if the attached device is not STP compatible.
PD4-572877743	The ExtremeXOS implementation of the Multiple Spanning Tree Protocol (MSTP) supports a revision level of 1 to 3, whereas other third party vendors support a revision level of 0 to 65535.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-12

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-12. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 52: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-539428440	In some cases, traffic ingressing an I/O module is not egressing out load shared ports whose member ports are on a different I/O module.
PD4-488646747	FDB entries are not learned for traffic that hits a service VLAN ID (SVID) translation policy.
Network Login	
PD4-399104181	When netlogin is configured with multiple authentication protocols on the same port, the authentication response from one protocol should not override the already authenticated state of a client.
PD4-466032303	If the encrypted password entered for the CLI command `configure netlogin add mac-list <mac> encrypted` contains the "<" characters, the configuration fails.
QoS	
PD4-397774546	vMAN egress ACL with Class of Service (C-COS) in match condition is resulting in unexpected behavior.
SNMP	
PD4-481623940	Simple Network Management Protocol (SNMP) authentication failure traps do not include IP address details, that is, the IP address from which the authentication attempt was made.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-10

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-10. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 53: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-443273921, PD4-438482687	When Protocol Independent Multicast (PIM) receives a prune from a downstream neighbor, the prune hold time is not considered. This is the time for which the upstream neighbor should hold the prune.
PD4-443273938, PD4-438482713	When creating a (S,G) entry from a (*, G) entry, start the entry timer based on the (*, G) egress hold time.
PD4-443273984, PD4-438482720	When a (*, G) entry is removed, the hold timer should be restarted for the next maximum hold time.
PD4-443515354, PD4-438482695	Protocol Independent Multicast (PIM) cache timeout should not be determined by the configured join/prune interval on a VLAN.
PD4-402030777	Issuing the `show log match ||` command causes the emsServer process to crash with a signal 6 error.
PD4-446885541	On rare occasions, the authentication, authorization, and accounting (AAA) process dies with signal 6 due to an assertion failure while authenticating an SSH user using TACACS+.
PD4-376341922	Making web-based calls using HTTP on an ExtremeXOS switch causes the switch to increase AAA memory utilization.
PD4-522345204, PD4-328163465	CPU utilization increases up to 99.9% when SNMP polls the extremeFdb MIB and generates the following error message: `08/08/2008 18:27:36.45 MSM-A: CPU utilization monitor: process fdb consumes 99 % CPU`
PD4-443927611	Traffic does not egress a 10G4Xc or 10G8Xc module with load sharing enabled.
BlackDiamond 10808 Switch	

PD4-449877739, PD4-411932475	A BlackDiamond 10808 switch with an I/O module goes into a failed state and displays the following error in the system log:
	`MSM-A: Slot-6 FAILED (1) L2 ping thru MSM-A timeout`
	`MSM-A: Slot-2 FAILED (1) L2 ping thru MSM-A timeout`
	`MSM-A: Slot-2 FAILED (1) Control link ping timeout`

ARP	
PD4-412404954	After an MSM failover, a BlackDiamond 8800 switch with a 10G8X module does not process client initiated address resolution protocol (ARP) requests. If you remove and then reinsert the backup MSM after the failover, the ARP requests are processed correctly.
Multicast	
PD4-468874495, PD4-461246875	Multicast manager is showing continuously increasing memory consumption.
PD4-449901506	Disabling multicast flooding on a port may result in ARP requests being blocked.
Spanning Tree Protocol	
PD4-453116841	Spanning Tree Protocol (STP) BPDUs are filtered on a per-port basis instead of a per-VLAN basis.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-7

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-7. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 54: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-485801147	BlackDiamond 8806 and 8810 I/O modules may reset without an external trigger.
IGMP	
PD4-473100155	IP packets sent to local multicast group 224.0.0.x may occasionally be slow path forwarded, even with IGMP snooping disabled.
Network Login	
PD4-441418181	Using MAC-based network login, the MAC address is authenticated on the first VLAN only. The same MAC address stays in the unauthenticated state in all other subsequent VLANs.
PD4-476352155	The error message that is logged when adding a port as untagged in more than one VLAN is more user friendly.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-4

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-4. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 55: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-419725145, PD4-459489323	A Summit X250e-48t stack generates the following error message each time a user is authenticated through MAC-based network login from the backup switch in the stack: `Unable to get vpif information IPmc add port.`
PD4-459420351, PD4-337044674	A defective Power over Ethernet (PoE) module may cause a switch to continuously reboot.
PD4-463217627, PD4-463217728	Hardware Abstraction Layer (HAL) memory shows a significant increase when refreshing a policy.
PD4-359462827	Process AAA dies if a Vendor Specific Attribute (VSA) with a length greater than 130 bytes is included in a RADIUS packet.
SummitStack	
PD4-441118181, PD4-453897651	Clients connected to a front panel port of a backup slot in a SummitStack cannot, in some case, communicate (ARP, ping) with the switch. This issue occurs only when load sharing is configured on ExtremeXOS switches using the ports from backup slots.

Table 55: Platform-Specific and Feature PDs (Continued)

CLI	
PD4-428888970, PD4-444518321	Logging out of a CLI session established using SSH or Telnet may result in a `smbuf_xfer:terminal signal` error followed by a switch reboot.
ELRP	
PD4-454742244	When running the Extreme Loop Recovery Protocol (ELRP) between an ExtremeWare "e" series switch and an ExtremeXOS switch, the ExtremeWare switch reports a checksum error.
IGMP	
PD4-409050568	When adding a static Internet Group Management Protocol (IGMP) group to a port not belonging to the assigned VLAN, the switch silently drops the configuration without displaying an error or warning message.
Multicast	
PD4-461646362	With Multicast VLAN Registration (MVR) enabled on a switch, adding or deleting a port from a non-MVR VLAN results in the multicast entries being flushed or refreshed. This is seen with Internet Group Management Protocol (IGMP) snooping as the ages of the incoming streams are reset to 0.
Network Login	
PD4-461738214, PD4-457325458, PD4-461738253	When a network login authentication method is enabled globally (`enabled netlogin <dot1x|mac|web>`) on a port for the first time, all the FDB entries corresponding to that port are not getting flushed.
SNMP	
PD4-457325663	The SNMP Object Identifier (OID) extremeVlanIfadminstatus used to disable a VLAN in ExtremeXOS returns an error. However, enabling a VLAN from a disabled state is functioning correctly.
PD4-360182229, PD4-457325601	The Simple Network Management Protocol (SNMP) does not respond to an snmpwalk after adding a trapreceiver if a community name starts with a `v`. If the community name begins with a `v` and has more than one character, the switch does not respond. However, the switch responds if the community name is only `v`.

Resolved Issues in ExtremeXOS 12.1.2.17-patch1-3

The following issues were resolved in ExtremeXOS 12.1.2.17-patch1-3. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 56: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-386193795, PD4-379068411	To avoid false warnings such as `<Warn:HAL.IPv4Adj.RmtHostL3TblFull> MSM-A: IPv4 unicast remote host entry not added. Hardware L3 Table full` from appearing in the log the following changes have been implemented: • Avoid a timing window where a new route is learned around the same time a new remote host is sampled. • Do not perform remote host sampling on packets sent to the CPU for L2 software learning (such as MAC limit-learning), or packets whose source MAC is not that of the switch. • Prevent warning messages for duplicate add of an existing remote host.
PD4-389339527	A netTools process crash occurs when processing incoming BOOTP Reply when User Datagram Protocol (UDP) forwarding is enabled.
BlackDiamond 8800 Series Switch	

PD4-354784718	On a BlackDiamond 8800 series switch, the following error appears in the syslog prior to seeing a “hal” crash on the switch:
	`MSM-A: Unknown cardtype in slot 9 - please program the eeprom`
	`MSM-A: ahd_eeprom_read: Error reading eeprom for slot 9 at offset 0`

ACL	
PD4-362643617	Refreshing an egress vMAN translation ACL with the keyword deny removed as an action modifier, or unconfiguring the egress ACL itself, causes all traffic ingressing a port to be dropped.
PD4-307360639	An abstract warning message is printed on a port being added as a tagged port in a learning-domain when it is untagged in a different vMAN and vice versa.
PD4-309933739	Configuring a vMAN ACL with invalid action modifiers does not show any errors.
Spanning Tree Protocol	
PD4-418743606, PD4-332966643	Adding a VLAN to STP domain (s0) and then enabing STP domain (s0) generates the following error: `Error: Incorrect carrier vlan configuration of port 2 in stp domain s0.` If you enable STP domain (s0) first and then add the VLAN to the STP domain, the configuration is accepted. **Workaround:** Enable the STP domain first and then add the VLAN.

Resolved Issues in ExtremeXOS 12.1.2.17

The following issues were resolved in ExtremeXOS 12.1.2.17. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16 through patch1-13. For information on those fixes, see the release notes for the specific release.

Table 57: Platform-Specific and Feature PDs

PD Number	Description
General	
PD4-334535100	Running the debug hal show version msm command generates the following system error on a BlackDiamond 8800 series switch with an MSM-48c in MSM-A slot: 08/14/2008 04:36:44.68 MSM-A: ahd_adm1066_cmd: Error reading ADM1066 for slot 11 rc=-1
PD4-281874747, PD3-192013071	The `disable jumbo-frame ports` command is allowed on Summit switches and BlackDiamond 8800 module ports, with the exception of original Summit X450 series switches and original BlackDiamond 8800 modules. On all other Summit switches and BlackDiamond 8800 modules, the command is properly executed but the configuration is not saved across switch reboots.
PD4-300801557	The following erroneous Event Management System (EMS) message is displayed even when the memory level of a switch is at a safe level: `07/15/2008 05:12:23.91 MSM-A: aspenHCErrorHandler: Card 2 is low on OS Memory. KBytes Total/Free = 110208 / 16040.`
PD4-266013210, PD3-192633919	A switch experiences an async queue deadlock, which is followed by memory depletion.
PD4-328904792	On a Summit X450a series switch, software redundant ports work correctly even after multiple link flaps.
PD4-294933687	Connectivity Fault Management (CFM) prematurely reports a connectivity fault before initializing I/O modules and links. A remote end-point is reported as expired during boot-up, which is logged before a link to the remote end-point is brought up.
PD4-286201111	When performing a PIM-SM performance test using 4,096 (*,G) groups, the following error is displayed: `hal: Reached maximum otp index allocation`
PD3-209052145, PD3-209042091	When two 100BASE-T FX and FX/LX GBICs are inserted in a Summit X450, and some of the links are between a BlackDiamond 8800 and the Summit X450, if the 100FX is disabled and rebooted, multiple ports of the Summit X450 no longer display in the `show ports configuration` command output.
BGP	
PD3-211438941, PD4-245719933	When downgrading a switch from ExtremeXOS 12.1 to an earlier version of ExtremeXOS software, it is recommended that you disable the unicast and multicast capabilities of BGP after the downgrade.
DHCP	
PD4-289525161	When DHCP snooping is enabled, bursts of DHCP traffic may cause exceptions (system crash) in the DHCP snoop module.
Diagnostics	
PD3-74554921	System health check related configurations are not stored in uploaded configurations.

Table 57: Platform-Specific and Feature PDs (Continued)

EAPS	
PD3-203480721	When a BlackDiamond 10808 or BlackDiamond 12800 series switch is configured as an EAPS controller in a scaled environment consisting of 130 or more EAPS domains, 4,000 protected VLANs, and 200,000 or more FDB entries, the failure or restoration of the EAPS common-link may cause a short network loop.
PD3-202013003	When an EAPS shared-port controller or partner switch reboot, when the shared-port (LACP) is active, but the shared-port status is still blocking, a temporary loop and broadcast storm occurs.
IS-IS	
PD3-194507463	Multiple L1/L2 routers in the same L1 area with at least one non-overlapping area address, incorrectly installs default routes to each other.
MAC-in-MAC	
PD3-189838058	Traffic is forwarded through a BVLAN even if the BVLAN is disabled.
MPLS	
PD3-209423226	VPLS goes into SGNL state after changing VPLS to take RSVP LSP from static LSP as a transport LSP. **Workaround:** Disable and enable MPLS to bring up VPLS.

PD3-202006051	Quickly executing the following pairs of configuration commands may cause errors. On a single MSM, the second command is rejected and an error is printed. On a dual MSM, the command may pass on the backup MSM and then fail on the primary MSM, resulting in an out-of-sync condition.
	`disable igmp snooping vlan myvlan`
	`configure vpls myvpls add service vlan myvlan`
	`configure vpls myvpls delete service myvlan`
	`enable igmp snooping vlan myvlan`
	Workaround: Pause between issuing the commands. If the problem occurs on a single MSM, re-enter the last command. If the problem occurs on a dual MSM, the last command will need to be undone (for example, `configure vpls myvpls delete service myvlan` or `disable igmp snooping vlan myvlan`), and re-entered.

PD3-116409584	When enabling the LDP loop detection feature, the path vector TLVs LSR-IDs are not updated. To workaround this issue, disable and enable MPLS.
PD3-116640291	LDP path vector loop detection may not perform as expected. For example, the LSR can advertise and propagate path vector TLVs, but will not reject FECs whose path vector value exceeds the configured path vector limit.
Multicast	

PD4-325245190	The following message is shown in the log without stating which message was suppressed:
	`07/21/2008 20:13:48.38 Slot-1: NET: 7697 messages suppressed.`
	`07/21/2008 20:13:53.38 Slot-1: NET: 8789 messages suppressed.`
	The log should also show which message was suppressed.

PD4-276815768	Enabling PIM snooping on a vMAN causes duplication of PIM control packets.
PD4-234942701	After a switch with PIM snooping enabled receives a PIM packet that includes the DR option, the multicast manager process dies.
PD4-275662331	A multicast stream on a vMAN running PIM snooping intermittently stops. As a result, the PIM snooping entries are being flushed after the hold timer (105) expires, even though there is a PIM hello exchange.

Table 57: Platform-Specific and Feature PDs (Continued)

PD3-210637311	Using MVR on a Summit and BlackDiamond 8800 a-series, e-series, or c-series platforms configured with tagged subscribing VLANs may cause unexpected untagged packet forwarding and error level log messages such as: `06/09/1920 00:08:49.87 <Erro:Kern.IPv4Mc.Error> Slot-8: Unable to Del IPmc vlan 210 for 8:1 s,G=c1010104,e101000a IPMC 9, unit 0 Entry not found` **Workaround:** Assign an IP interface to each tagged subscriber VLAN.
PD3-209983742	When a slot on a BlackDiamond 8800 or SummitStack switch reboots with active Layer-3 IP multicast subscribers, traffic will not resume until the IP multicast cache is flushed and relearned.
PD3-208735701	Removing a PIM VLAN from a PIM domain using the `configure pim delete vlan <vlan name>` command and adding the VLAN back into the PIM domain using the `configure pim add vlan <vlan name> sparse` command does not restore traffic on a remote MSDP domain. Explicitly disable PIM and enable PIM to restore traffic.
PD3-206283185	When PIM snooping is enabled both globally and on a VLAN, disabling PIM snooping on the VLAN also disables PIM snooping globally.
PD3-163090651	No error messages are displayed when unconfiguring a group limit on a port that does not have a group limit configured.
PD3-168968151	When configuring IGMP, the maximum response time can be configured to a higher time interval that the query response time without the system displaying a warning message that this is not allowed.
PD3-171281681	PIM Layer 3 multicast forwarding is not working properly on a private VLAN with PIM enabled in dense mode.
PD3-177958011, PD3-201244849	A switch configured for MVR leaks multicast packets to VLANs that are not configured to receive multicast streams.
Network Login	
PD3-204414763	When a switch is up and running and all ports are in a default VLAN, the switch does not forward an EAPOL frame from a supplicant.
Network Services	
PD3-65450031	When configuring and applying a certain ingress ACL, traffic stops forwarding to ports belonging to the same vMAN. Removing the ingress ACL restores traffic.
OSPF	
PD3-202839989	Static routes advertised to OSPF are lost after restarting OSPF when graceful restart is enabled
PoE	

PD4-283661276	A false alarm is occasionally generated even though the measured power is well below the power usage threshold.
	`07/28/2008 07:27:05.33 <Noti:POE.power_cleared> Power usage threshold condition cleared, slot 1`
	`07/28/2008 07:27:03.12 <Warn:POE.power_exceeded> Power usage exceeding threshold for slot 1`
	`07/28/2008 07:27:00.92 <Noti:POE.power_cleared> Power usage threshold condition cleared, slot 1`
	`07/28/2008 07:26:56.51 <Warn:POE.power_exceeded> Power usage exceeding threshold for slot 1`

SNMP	
PD4-264761905	The Object Identifier (OID) for a Summit X150-24 is missing from the MIB files. The OID should have the form 1.3.6.1.4.1.1916.2.xx. If you upload the MIB file to an SNMP browser, all system identifiers are shown except for the Summit X150.
PD4-217023403	Traps can now be sent to trap receivers on VR-Default even when the default gateway is configured on VR-Mgmt.

Table 57: Platform-Specific and Feature PDs (Continued)

Spanning Tree Protocol	
PD4-228364771	A connection loss can occur when a boundary port transitions to a blocking state at the multiple spanning tree instance (MSTI) level when `edge-safeguard` is enabled.
SSL	
PD3-29939091	ssh.xmod must be installed to configure SSL certificates. If ssh.xmod is not installed on the switch, configured SSL certificates are not loaded into the switch and no error is returned.
PD3-29034131	Saving an SSL configuration causes temporary high CPU utilization.
Stacking	
PD3-126815409	The `configure sys-recovery-level slot` command does not currently work on stack slots.
Rate Limiting	
PD4-291186891, PD4-306886471	Beginning with ExtremeXOS 12.1 or later, traffic reaching the egress rate limiting queue may be dropped.
Wireless	
PD3-205447934	Enabling `ip-security anomaly-protection` with the "l4port" option, which is also included in the default options when no option is specified, prevents a wireless AP from being registered with Summit WM controllers.

Resolved Issues in ExtremeXOS 12.1.1.4

The following issues were resolved in ExtremeXOS 12.1.1.4. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16. For information on those fixes, see the release notes for the specific release.

Table 58: Platform-Specific and Feature PDs

PD Number	Description
General	
PD3-187495081	Traffic switching performance drops by 50% to 90% when an MSM failover occurs between SVLANs and BVLANs.

PD3-180718721	When booting a dual MSM system, the following error message may be displayed in the log for MSM A and MSM B. This error message only applies to MSM B:
	On MSM A:
	`* BD-12804.3 # show log severity error`
	`11/07/2007 20:54:24.34 <Erro:DM.Error> MSM-B: Other MSM is 9 ??`
	On MSM B:
	`BD-12804.1 > show log severity error`
	`11/07/2007 20:54:24.34 <Erro:DM.Error> MSM-B: Other MSM is 9 ??`

BlackDiamond 8800 Series Switch	
PD3-151784861	10G4Ca modules on BlackDiamond 8800 platforms may require custom pre-emphasis settings on an interface by interface basis as some vendor cables and end devices require custom settings to operate without CRC errors.

Table 58: Platform-Specific and Feature PDs (Continued)

PD Number	Description
BlackDiamond 10808 Switch	
PD3-36734601	The Opnext ZR XENPAK module is displaying as an SR module on the BlackDiamond 10808 switch.
PD3-37075321	The Intel ER and Intel LR XENPAK modules are displaying as SR modules or unsupported on the BlackDiamond 10808 switch.
BlackDiamond 12800 Series Switches	
PD3-180903136, PD3-205448322	BlackDiamond 12800 series switches are not compatible with ExtremeXOS versions 11.6 or earlier. It is recommended that these switches be loaded with ExtremeXOS 12.0 or later.
PD3-151784861	10G4Ca modules on BlackDiamond 8800 platforms may require custom pre-emphasis settings on an interface by interface basis as some vendor cables and end devices require custom settings to operate without CRC errors.
Summit Family of Switches	
PD4-890754513	The error message `Operation attempted to set two rules of identical conditions with the same precedence` is seen when applying two different policies to two different VLANs.
PD3-179276997	Running the `show ports information` and `show ports configuration` commands on a Summit switch that does not include an XGM2 option card erroneously displays the ports on the card as available and enabled.
ACL	
PD3-28320337	MAC and IP MAC entries are being allowed in the same IPv6 ACL rule entry. L2 and L3/L4 rules should not be allowed in one entry; this should fail the grammar check but does not.
PD3-55929951, PD3-41829516	The keyword `icmp-type timestamp` when used in an ACL policy match condition does not work. Using the ICMP number code instead of the keyword works correctly (icmp-type 13).
PD3-28320337	MAC and IP MAC entries are being allowed in the same IPv6 ACL rule entry. L2 and L3/L4 rules should not be allowed in one entry; this should fail the grammar check but does not.
PD3-42872248	Creating dynamic ACLs using the operands "<" or "<=" results in an error. Use "lt" and "lte" instead.
PD3-42447111, PD3-166801770	The ACL action mirror-cpu and log do not work.
PD3-56605924	Multiple egress vMAN ACL rules with identical IF-conditions but different egress ports cannot be distinguished. Packets are going to be forwarded based on only one of the applicable rules.
BGP	
PD3-41952658	BGP traps transmitted from a BlackDiamond or Summit X450 switch are missing the peer IP addresses.
CLEAR-Flow	
PD3-95652911, PD3-95652994	When using the `show clear-flow` command, RL is not included in the Threshold Type with CN, DT, and DR.
Control Protocols	
PD3-84477402, PD3-75421071	When creating a CIST domain and then configuring the link-type as point-to-point for CIST, the link-type configuration is lost when the uploaded configuration is downloaded.
Documentation	
PD3-201780134	The ethernet-source-address mask is not supported in ExtremeXOS 12.0 as stated in the *ExtremeXOS 12.0 Concepts Guide*. It is supported in ExtremeXOS 12.1.

Table 58: Platform-Specific and Feature PDs (Continued)

PD Number	Description
EAPS	
PD3-176462601	EAPS takes approximately 120 milliseconds to 160 milliseconds to recover after restoring a link failure.
PD3-86015057	The following error message is displayed in the log when disabling port sharing on ring ports: `08/01/2006 19:49:32.55 <Crit:vlan.err.criticalInfo> Critical Info: handleVMngrProtoIfSetState procName:eaps protolId:0x80 not registered vpif->l2Protos:0x0, vpif:1:4 on pv50 ingress:0x5 egress:0x1 dereg:0 (0 of 50)s`
PD3-86015166	When LACP is enabled on a link between two switches, when disabling port sharing, the following warning is displayed in the log for each of the protected VLANs: `08/02/2006 12:20:31.36 <Warn:EAPS.SharedPort.SegPortWarning> EAPS Shared-port 4, Segment-port 4 - No vPif for vlan pv24`
PD3-96983520	Changing the EAPS shared port link ID of a partner/controller pair while there is a failure in the EAPS network is not recommended and may cause a loop in the network.
PD3-131018386	After changing the root blocker and partner IDs, the displayed root blocker ID toggles between the original and the changed IDs.
PD3-135517703, PD3-87003427, PD3-78960443, PD3-78302829	Configurations having three shared links, where the shared link with the lowest ID is in the middle, the root blocker marks the segment as "blocking-down," but the ports are not in a blocked state. To get out of the loop, restore the shared links. To avoid encountering this condition, insure that no more than two shared links become disabled.
IP Unicast	
PD3-192315271, PD3-182815070	When a switch is configured for proxy ARP with the `always` keyword, the switch will not respond to a gratuitous ARP request, it will only respond to ARP requests.
MPLS	
PD3-167174547	The command output for the `show vpls peer detail` command does not show the peer flags.
PD3-114261166	Port flapping, and other problems, can cause logs similar to the following when 802.1Q tagged packets are software forwarded for a VPLS service VLAN: `12/15/2006 08:11:40.67 <Erro:Kern.Error> MSM-A: nettx_vpls_transmit.(987) VPLS - problems determining .1q tag for encapsulated packet.` The logs are the result of other problems such as port flapping and will no longer appear when the other problems are corrected.
PD3-117148339	Enabling or disabling penultimate hop popping on a VLAN does not work if MPLS is enabled.
PD3-169466471	The `show fdb vpls <vpls_name>` command shows the entire FDB entry.
PD3-179426902, PD3-188166267, PD3-177361681	Existing MPLS forwarding data is not installed on newly inserted BlackDiamond 12800 series switches, which can cause problems when receiving and transmitting MPLS packets on those I/O modules. **Workaround:** Disable and enable MPLS.
PD3-135927701	The `show vpls detail` command does not display the updated counters (RX Pkt and RX Bytes) when using “q” to quit. The counters are updated after running the complete command.
PD3-88153931	The ExtremeXOS route table and kernel route table show that an LSP next hop for a specific route is available. However, when `ping` or `traceroute` commands are run for a destination reached by the route, the LSP next hop may not be used.

Table 58: Platform-Specific and Feature PDs (Continued)

PD Number	Description
Network Services	
PD3-42385251,	When creating a large policy file on a BlackDiamond 10808 switch and applying the policy to a VLAN on egress, if traffic is sent that attempts to hit the ACL rules, and the next hop ARP entry is not yet learned, the MSMs may stop responding.
vMAN	
PD3-203983381	In ExtremeXOS 12.0.3, when a BVLAN tag is changed, a packet egressing the BVLAN does not reflect the changed tag. Packets still egress the BVLAN using the original tag. This problem applies to all vMANs (create vman, create bvlan, and so on) and occurs only if the BVLAN tag is changed and the BVLAN contains ports. This does not apply to a BVLAN that is created without any ports. **Workaround:** Save the configuration and reboot the system.

Resolved Issues in ExtremeXOS 12.1.0.29

The following issues were resolved in ExtremeXOS 12.1.0.29. The numbers shown in column one of the following table are for internal reference and can be ignored. ExtremeXOS 12.1 includes all fixes up to and including ExtremeXOS 11.1.4.4, ExtremeXOS 11.2.3.3, ExtremeXOS 11.3.4.5, ExtremeXOS 11.4.4.7, ExtremeXOS 11.5.2.10, ExtremeXOS 11.6.4.11 through patch1-8, and ExtremeXOS 12.0.3.16. For information on those fixes, see the release notes for the specific release.

Table 59: Platform-Specific and Feature PDs

PD Number	Description
MPLS	
PD3-188165546, PD3-120757801	On BlackDiamond 12800 series switches, received MPLS packets for which an MPLS label lookup is performed are not mirrored when ingress mirroring is activated.